

Sets, the Axiom of Choice, *and all that*: A Tutorial

Ernst-Erich Doberkat
Chair for Software Technology
Technische Universität Dortmund
`ernst-erich.doberat@udo.edu`

September 1, 2014

Abstract

This tutorial deals with the application of the Axiom of Choice in one of its popular disguises to objects which are of some interest in computer science (like lattices, Boolean algebras, filters and ideals, games). We discuss some common variants of this axiom such as Zorn's Lemma, Tuckey's Maximality Principle, the Well-Ordering Theorem and the Maximal Ideal Theorem; each equivalence gives applications its due attention. We show that the Axiom of Choice can be used to demonstrate the existence of non-measurable sets in the real line. This is an occasion to introduce some measure theory within the context of Boolean σ -algebras.

Games are introduced as well, and the Axiom of Determinacy is discussed, giving rise to show that this axiom can be used to demonstrate that each subset of the real line is measurable. Hence we use games as a tool for proofs. We try to shed some light on the slightly complicated and irritating interplay between these two axioms.

We assume the basic knowledge of mathematics that is introduced by a one year course for beginning computer scientists at a German university. A grain of mathematical maturity may help as well. Some exercises are offered, and solutions are suggested as well.

Contents

1	The Axiom of Choice and Some Of Its Equivalents	2
1.1	The Axiom of Choice	7
1.2	Cantor's Enumeration of $\mathbb{N} \times \mathbb{N}$	8
1.3	Well-Ordered Sets	11
1.4	Ordinal Numbers	15
1.5	Zorn's Lemma and Tuckey's Maximality Principle	21
1.5.1	Compactness for Propositional Logic	22
1.5.2	Extending Orders	25
1.5.3	Bases in Vector Spaces	26
1.5.4	Extending Linear Functionals	27
1.5.5	Maximal Filters	29
1.5.6	Ideals and Filters	31
1.5.7	The Stone Representation Theorem	35
1.5.8	Compactness and Alexander's Subbase Theorem	38
1.6	Boolean σ -Algebras	43
1.6.1	Construction Through Transfinite Induction	47
1.6.2	Factoring Through σ -Ideals	48
1.6.3	Measures	49
1.6.4	μ -Measurable Sets	59
1.7	Games	61
1.7.1	Determined Games	62
1.7.2	Proofs Through Games	64
1.8	Wrapping it up	70
1.9	Bibliographic Notes	70
1.10	Exercises	72
1.11	Solutions	75
	References	81

1 The Axiom of Choice and Some Of Its Equivalents

Sets are a universal tool for computer scientists, the tool which has been imported as a *lingua franca* from mathematics. Program development, for example, starts sometimes from a mathematical description of the things to be done, the specification and the data structures and — you guess it — sets are the language, in which these first designs are usually written down. There is even a programming language called **SETL** based on sets [SDDS86], this language served as a prototyping tool and was essentially motivated by the ambition to make the road from a formal description of an object to its representation through an executable program as short as possible [DF89].

In fact, it turned out that programming in what might be called executable set theory has the advantage of being able to experiment with the objects at hand, leading, for example to the first implementation of the programming language **Ada**, the implementation of which was deemed for quite a long time as nearly impossible. On the other hand it turned out that sets may be a feature nice to have in a programming language, but that they are probably not always the appropriate universal data structure for engineering program systems; this is witnessed by the fact that some languages, like for example **Haskell**[OGS09], have set-like constructs such as list comprehension, but they do not implement sets fully. As the case may be, sets are important objects when arguing about programs, they constitute an important component of the tool kit which a serious computer scientist should have ready in his backpack.

When surveying the computer science literature, we see that sets and the corresponding constructs like maps, power sets, orders etc. are being used freely, but there is usually no concern regarding the axiomatic basis of these objects — sets are being used, albeit in a fairly naive way. This should not surprise anybody, because they are just tools and most of the time not the objects of consideration themselves. A tool should be handy and come to the use of a computer scientist as soon as needed, but it really should not bring with it complications of its own. Fairly early in the education of the computer scientist, however, she or he encounters the phenomenon of recursion, be it as a recursive function, be it as a recursive definition. And here of course the question arises immediately, why the corresponding constructs work, specifically, how one can be sure that a particular recursive program is actually terminating. The same question, probably a little bit more focused, appears in techniques which are related to term rewriting. Here one inquires whether a particular chain of replacements will actually lead to a result in a finite amount of time. People in term rewriting have found a way of writing this down, namely a terminating condition which is closely related to some well-ordering. This means that we do not have infinitely long chains; this is of course a very similar condition to the one that is encountered when talking about the termination of a recursive procedure: Here we do not want to have infinitely long chains of procedure or method calls. This suggests structural similarities between the invocation of a recursive method terminates, and rewriting a term. If you think about it, mathematical induction enters this family of observations, the members of which show a considerable similarity.

When we investigate the background in front of which all this happens, we find that we need to look at well-orderings. These are orderings which forbid the existence of infinitely long decreasing chains. It turns out that the mathematical ideas expressed here are fairly closely connected to ordinal numbers. It is not difficult to construct a bridge from orderings and well-

orders to the question whether it is actually possible to find a well-order for each and every set. The bridge a computer scientist might traverse is loosely described as follows: Because we want to be able to deal with arbitrary objects, and because we want to run programs over these arbitrary objects, it should be possible to construct terminating recursive methods for those objects. But in order to do that, we should make sure that no infinite chains of method invocations may occur, which in turn poses the question whether or not we can impose an order on these objects that renders infinite chains impossible (admittedly somewhat indirectly, because the order is imposed actually by procedure calls). But here we are — we want to know whether such a construction is possible; mathematically this leads to the possibility of well-ordering each and every set.

This question is of course fairly easy to answer when we talk about finite scenarios, but sometimes it is mandatory to consider infinite objects as well. The world may be finite, but our models of the world are not always. Hence the question arises whether we can take an arbitrarily large set and construct a well-ordering for this set. As it turns out, this question is very closely connected to another question, which at first glance does not really look similar at all: We are given a collection of non-empty sets, are we able to select from each set exactly one element? This question has vexed mathematicians for more than one century now. One of the interesting points which indicates that things are probably a little bit more complicated than they look is the observation that the possibility of well-ordering arbitrary set is equivalent to the question of selection, which came to be known as the Axiom of Choice. It turned out during the discussion in mathematics that there is really a whole and very full bag of other properties, which are equivalent to this axiom. We will see that the Axiom of Choice is equivalent to some well-known proof principles like Zorn's Lemma or Tuckey's Maximality Principle. Because this discussion relating the Axiom of Choice and similar constructions has been raging in mathematics for more than one century now, we can not hope to be able to even completely list all those things which we have to leave out. Nevertheless we try to touch upon some topics, which appear to be important for developing mathematical structures within computer science.

Since the Axiom of Choice and its variants touch upon those topics in mathematics much in use in computer science, this gives us the opportunity to select some of these topics and discuss them, independently and in the light of the use of the Axiom of Choice. We discuss for example lattices, introduce ideals and filters and pose the maximality question: Is it always possible to extend a filter to a maximal filter? It turns out that the answer is in the affirmative, and this has some interesting applications for the structure theory of, for example, Boolean algebras. Because of this we are able to discuss one of the true classics in this area, namely Stone's Representation Theorem, which says that every Boolean algebra is isomorphic to an algebra of sets. Another interesting application of Zorn's Lemma is Alexander's Theorem, which shows that one may restrict one's attention to covering a topological space with subbase elements for establishing compactness of the space. Because we have then compactness at our disposal, we establish also compactness of the space of all prime ideals of a Boolean algebra. Quite apart from these question, which are oriented towards order structures, we establish the Hahn-Banach Theorem, which shows that a dominated linear functional can be extended from a linear subspace to the entire space in a dominated way.

A particular class of Boolean algebras are closed under countable infima and suprema, these algebras are called σ -algebras. Since these algebras are interesting in particular when it

comes to probabilistic models in computer science, we treat these σ -algebras in some detail, in particular with respect to measures and their extensions. The general situation in application is sometimes that one has the generator of a Boolean σ -algebra and a set function which behaves decently on this generator, and one wants to extend this set function to the whole σ -algebra. This gives rise to a fairly rich and interesting construction, which in turn has some connections to the question of the Axiom of Choice. The extension process extends the measure far beyond the Boolean σ -algebra generated by the family under consideration, and the question arises how far this extension really goes. This may be of interest, e.g., if one wants to measure some set, so that one has to know whether this set can be measured at all, hence whether it is actually in the domain of the extended measure. The Axiom of Choice helps in demonstrating that this is not always possible. It can be shown that there are sets which can not be measured. This depends on a selection argument for classes of an easily constructed equivalence relation.

This will be discussed. Then we turn to games, games as a model for human interaction, we have two players, Angel and Demon, playing against each other. We describe how a game is played, and what strategies are, in particular what constitutes winning strategies. This is done first in the context of infinite sequences of natural numbers. The model has the advantage of being fairly easy to grasp, it has the additional structural advantage that we can map many applications to this scenario.

Actually, games become really interesting when we know that one of the participants has actually a chance to win. Hence we postulate that our games are of this kind, so that always either Angel or Demon has a strategy to win the game. Unfortunately it turns out that this postulate, called the Axiom of Determinacy, is in conflict with the Axiom of Choice. This is of course a fairly unpleasant situation, because both axioms seem to be reasonable statements. So we have to see what can be done about this. We show that if we assume the latter axiom, we can actually demonstrate that each and every subset of the real line is measurable. This is a contradiction to the observation we just related.

This discussion serves two purposes. The first one is that one sometimes wants to challenge the Axiom of Choice in favor of other postulates, which may turn out to have more advantages (in the context of games, the postulate that one of the players has a winning strategy, no matter how the game is constructed, has certainly some advantageous aspects). But the Axiom of Choice is, as we will see, quite a fundamental postulate, so one has to find a balance between both. This does look terribly complicated, but on the other hand does not seem to be difficult to manage from a practical point of view — and computer scientists are by definition practical people! The second reason for introducing games and for elaborating on these results is to demonstrate that games can actually be used as tools for proofs. These tools are used in some branches of mathematics quite extensively, and it appears that this may be an attractive choice for computer scientists as well.

We work usually in what is called *naive set theory*, in which sets are used as a formal manner of speaking without much thinking about it. Sets are just tools to express formal thoughts.

When mathematicians and logicians like G. Frege, G. Cantor or B. Russell thought about the basic foundations of mathematics, they found a huge pile of unposed and unanswered questions about the basic building blocks of mathematics, e.g., the definition of a cardinal number was usually taken for granted, without a formal foundation; a foundation was even

resisted or ridiculed¹.

The Axioms of ZFC Nevertheless, at around the turn of the century there seems to have been some consensus among mathematicians that the following axioms are helpful for their work; they are called the *Zermelo-Fraenkel System With Choice (ZFC)* after E. Zermelo and A. A. Fraenkel.

We will discuss them briefly and informally now. Here they are.

Extensionality *Two sets are equal iff they contain the same elements.* This requires that sets exist, and that we know which elements are contained in them; usually these notions (set, element) are taken for granted.

Empty Set Axiom *There is a set with no elements.* This is of course the empty set, denoted by \emptyset .

Axiom of Pairs *For any two sets, there exists a set whose elements are precisely these sets.* From the extensionality axiom we conclude that this set is uniquely determined. Without the axiom of pairs it would be difficult to construct maps. Hence we can construct sets like $\{a, b\}$ and singleton sets $\{a\}$ (because the axiom does not talk about different elements, so we can form the set $\{a, a\}$, which, by the axiom of extensionality, equals the set $\{a\}$). We can also define an ordered pair through $\langle a, b \rangle := \{\{a\}, \{a, b\}\}$.

Axiom of Separation Let φ be a statement of the formal language with a free variable z . *For any set x there is a set containing all z in x for which $\varphi(z)$ holds.* This permits forming sets by describing the properties of their elements. Note the restriction “For any set x ”; suppose we drop this and postulate “There is a set containing all z for which $\varphi(z)$ holds.” Let $\varphi(z)$ be the statement $z \notin z$, then we would have postulated the existence of the set $a := \{z \mid z \notin z\}$ (is $a \in a$?). Hence we have to be a bit more modest.

Power Set Axiom *For any set x there exists a set consisting of all subsets of x .* This set is called the power set of x and denoted by $\mathcal{P}(x)$. Of course, we have to define the notion of a subset, before we can determine all subsets of a set x . A set u is called a subset of set x (in symbols $u \subseteq x$) iff every element of u is an element of x .

Union Axiom *For any set there is a set which is the union of all elements of x .* This set is denoted by $\bigcup x$. If x contains only a handful of elements like $x = \{a, b, c\}$, we write $\bigcup x$ as $a \cup b \cup c$. The notion of a union is not yet defined, although intuitively clear. We could rewrite this axiom a little by stating it as: given a set x , there exists a set y such that $w \in y$ iff there exists a set a with $a \in x$ and $w \in a$. The intersection of two sets a and b can then be defined through the axiom of separation with the predicate $\varphi(z) := z \in a \text{ and } a \in b$, so that we obtain $a \cap b := \{z \in a \cup b \mid z \in a \text{ and } a \in b\}$.

This is the first group of axioms which are somewhat intuitive. It is possible to build from it many mathematical notions (like maps with their domains and ranges, finite Cartesian

¹Frege’s position, for example, was considered in the polemic by J. K. Thomae, “Gedankenlose Denker, eine Ferienplauderei” (Thinkers without a thought, a chat for the vacations). Jahresber. Deut. Math. Ver. 15, 1906, 434 - 438 as somewhat hare-brained, see Thiel’s treatise [Thi65]

products). But it turns out that they are not yet sufficient, so an extension to them is needed.

Axiom of Infinity *There is an inductive set.* This means that there exists a set x with the property that $\emptyset \in x$ and that $y \cup \{y\} \in x$ whenever $y \in x$. Apparently, this permits building infinite sets.

Axiom of Replacement Let φ be a formula with two arguments. *If for every a there exists exactly one b such that $\varphi(a, b)$ holds, then for each set x there exists a set y which contains exactly those elements b for which $\varphi(a, b)$ holds for some $a \in x$.* Intuitively, if we can find for formula φ for each $a \in x$ exactly an element b such that $\varphi(a, b)$ is true, then we can collect all these elements b in a set. Let φ be the formula $\varphi(x, y)$ iff x is a set and $y = \mathcal{P}(x)$, then there exists for a given family x of sets the set of all powersets $\mathcal{P}(a)$ with $a \in x$.

Axiom of Foundation *Every set contains an \in -minimal element.* Sets contain other sets as elements, as we have seen, so there might be the danger that a situation like $a \in b \in c \in a$ occurs, hence that there is a \in -cycle. In some situations this might be desirable, but not in this very basic scenario where we try to find a fixed ground to work on. A formal description of this axiom reads that for each set x there exists a set y such that $y \in x$ and $x \cap y = \emptyset$. We will have to deal with a very similar property when discussing ordinal numbers in Section 1.4.

Now we have recorded some axioms which put the ground on our daily work, to be used without any qualms. It permits to build up the mathematical structures like relations, maps, injectivity, surjectivity, what have you. We will not do this here (it gets somewhat boring after a time if one is not after some special effect — then it may become awfully hard) but rather trust that these structures are available and familiar.

But there still is a catch: look at the argumentation in the following proposition which constructs some sort of an inverse for a surjective map.

Proposition 1.1 *There exists for each surjective map $f : A \rightarrow B$ a function $g : B \rightarrow A$ such that $(f \circ g)(b) = b$ for all $b \in B$.*

Proof For each $b \in B$, the set $f^{-1}[\{b\}]$ is not empty, because f is surjective. Thus we can pick for each $b \in B$ an element $g(b) \in f^{-1}[\{b\}]$. Then $g : B \rightarrow A$ is a map, and $f(g(b)) = b$ by construction. \dashv

WHERE IS THE CATCH? The proof seems to be perfectly innocent and straightforward. We simply have a look at all the inverse images of elements of the image set B , all these inverse images are not empty, so we pick from each of these inverse images exactly one element and construct a map from this.

Well, the catch lies in picking an element from each member of this collection. The collection of axioms above says nowhere that this selection is permitted (now you might think that mathematicians find a sneaky way of permitting such a pick, through the back door, so to speak; trust us — they cannot!).

Hence we need some additional device, and this is the Axiom of Choice. It will be discussed at length now; we take the opportunity to use this discussion as kind of a peg onto which

we hang some other objects as well. The general approach will be that we will discuss mathematical objects of interest, and at crucial point the discussion of (\mathbb{AC}) and its equivalents will be continued (if you ever listened to a Wagner opera, you will have encountered his leitmotifs).

1.1 The Axiom of Choice

The Axiom of Choice states that

(\mathbb{AC}) Given a family \mathcal{F} of non-empty subsets of some set X , there exists a function $f : \mathcal{F} \rightarrow X$ such that $f(F) \in F$ for all $F \in \mathcal{F}$.

The function the existence of which is postulated by this axiom is called a *choice function* on \mathcal{F} .

It is at this point not quite clear why mathematicians make such a fuss about (\mathbb{AC}) :

W. Sierpinski *It is the great and ancient problem of existence that underlies the whole controversy about the axiom of choice.*

P. Maddy *The Axiom of Choice has easily the most tortured history of all set-theoretic axioms.*

T. Jech *There has been some controversy about the Axiom of Choice, indeed.*

H. Herrlich *AC, the axiom of choice, because of its non-constructive character, is the most controversial mathematical axiom, shunned by some, used indiscriminately by others.*

In fact, let $X = \mathbb{N}$, the set of natural numbers. If \mathcal{F} is a set of non-empty subsets of \mathbb{N} , a choice function is immediate — just let $f(F) := \min F$. So why bother? We will see below that \mathbb{N} is a special case. B. Russell gave an interesting illustration: Suppose that you have an infinite set of pairs of shoes, and you are to select systematically one shoe from each pair. You can always take either the left or the right one. But now try the same with an infinite set of pairs of socks, where the left sock cannot be told from the right one. Now you have to have a choice function.

But we do not have to turn to socks in order to see that a choice function is helpful, we rather prove Proposition 1.1 again.

Proof (of Proposition 1.1)

Define

$$\mathcal{F} := \{f^{-1}[\{b\}] \mid b \in B\},$$

then \mathcal{F} is a collection of non-empty subsets of A , since f is onto. By assumption there exists a choice function $G : \mathcal{F} \rightarrow A$ on \mathcal{F} . Put $g(b) := G(f^{-1}[\{b\}])$, then $f(g(b)) = b$. \dashv

So this is a pure, simple and direct application of (\mathbb{AC}) , making one wonder what application the existence of a choice function will find. We'll see.

1.2 Cantor's Enumeration of $\mathbb{N} \times \mathbb{N}$

We will deal in this section with the comparison of sets with respect to their size. We say that two sets A and B have the same *cardinality* iff there exists a bijection between them. This condition can sometimes be relaxed by saying that there exists an injective map $f : A \rightarrow B$ and an injective map $g : B \rightarrow A$. Intuitively, A and B have the same size, since the image of each set is contained in the other one. So we would expect that there exists a bijection between A and B . This is what the famous Schröder-Bernstein Theorem says.

Theorem 1.2 *Let $f : A \rightarrow B$ and $g : B \rightarrow A$ be injective maps. Then there exists a bijection $h : A \rightarrow B$.*

Proof Define recursively

$$\begin{aligned} A_0 &:= A \setminus g[B], \\ A_{n+1} &:= g[f[A_n]] \end{aligned}$$

and

$$B_n := f[A_n].$$

If $a \in A$ with $a \notin A_0$, there exists a unique $b =: g^*(a)$ such that $a = g(b)$, because g is an injection. Now define the map $h : A \rightarrow B$ through

$$h(a) := \begin{cases} f(a), & \text{if } a \in \bigcup_{n \geq 0} A_n \\ g^*(a), & \text{otherwise.} \end{cases}$$

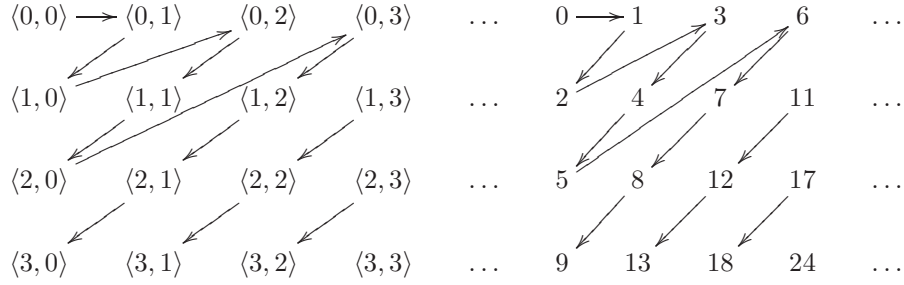
Assume that $h(a) = h(a')$. If $a, a' \in \bigcup_{n \geq 0} A_n$, we may conclude that $a = a'$, since f is one to one. If $a \in A_n$ for some n and $a' \notin \bigcup_{n \geq 0} A_n$, then $h(a) = f(a)$, $h(a') = g^*(a')$, hence $a' = g(h(a')) = g(h(a)) = g(f(a))$. This implies $a \in A_{n+1}$, contrary to our assumption. Hence h is an injection. If $b \in \bigcup_{n \geq 0} B_n$, then $b = f(a) = h(a)$. Now let $b \notin \bigcup_{n \geq 0} B_n$. We claim that $g(b) \notin A_n$ for any $n \geq 0$. In fact, if $g(b) \in A_n$ with $n > 0$, we know that $g(b) = g(f(a))$ for some $a \in A_{n-1}$, so $b = f(a) \in f[A_{n-1}]$, contrary to our assumption. Hence $h(g(b)) = g^*(g(b)) = b$. Thus h is also onto. \dashv

Another proof will be suggested in Exercise 7 through a fixed point argument.

Call a set A *countably infinite* there exists a bijection $A \rightarrow \mathbb{N}$. By the Schröder-Bernstein Theorem 1.2 it then suffices to find an injective map $A \rightarrow \mathbb{N}$ and an injective map $\mathbb{N} \rightarrow A$. A set is called *countable* iff it is either finite or countably infinite.

We will have a closer look at countably infinite sets now and show that the set of all finite sequences of natural numbers is countable; for simplicity, we work with $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

We start with showing that there exists a bijection from the Cartesian product $\mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0$. Cantor's celebrated procedure for producing an enumeration for $\mathbb{N}_0 \times \mathbb{N}_0$ works for an initial section as follows



Define the function

$$J(x, y) := \binom{x + y + x}{2} + x,$$

then an easy computation shows that this yields just the enumeration scheme of Cantor's procedure. We will have a closer look at J now; note that the function $x \mapsto \binom{x}{2}$ increases monotonically.

Proposition 1.3 $J : \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0$ is a bijection.

Proof 1. J is injective. We show first that $J(a, b) = J(x, y)$ implies $a = x$. Assume that $x > a$, then x can be written as $x = a + r$ for some positive r , so

$$\binom{a + r + y + 1}{2} + r = \binom{a + b + 1}{2},$$

hence $b > r + y$, so that b can be written as $b = r + y + s$ with some positive s . Abbreviating $c := a + r + y + 1$ we obtain

$$\binom{c}{2} + r = \binom{c + s}{2}.$$

But because we have $r < c$, we get

$$\binom{c}{2} + r < \binom{c}{2} + c = \binom{c + 1}{2} \geq \binom{c + s}{2}.$$

This is a contradiction. Hence $x \leq a$. Interchanging the rôles of x and a one obtains $a \leq x$, so that $x = a$ may be inferred.

Thus we obtain

$$\binom{a + y + 1}{2} = \binom{a + b + 1}{2}.$$

This yields the quadratic equation

$$y^2 + 2ay - (b^2 + 2ab) = 0$$

which has the solutions b and $-(2a + b)$. If $a = b = 0$ then $y = 0 = b$, if $b > 0$, the only non-negative solution is b , so that $y = b$ also in this case. Hence we have shown that $J(a, b) = J(x, y)$ implies $\langle a, b \rangle = \langle x, y \rangle$.

2. J is onto. Define $Z := J[\mathbb{N}_0 \times \mathbb{N}_0]$, then $0 = J(0, 0) \in Z$ and $1 = J(0, 1) \in Z$. Assume that $n \in Z$, so that $n = J(x, y)$ for some $\langle x, y \rangle \in \mathbb{N}_0$. We consider these cases

$$y > 0 : n + 1 = J(x, y) + 1 = \binom{x+y+1}{2} + x + 1 = J(x+1, y-1) \in Z.$$

$$y = 0 : n = \binom{x}{2} + x = \binom{x+1}{2}, \text{ thus } n + 1 = \binom{x+1}{2} + 1.$$

$$x > 0 : n + 1 = \binom{x+1}{2} + 1 = \binom{1+(x-1)+1}{2} + 1 = J(1, x-1) \in Z.$$

$$x = 0 : \text{ Then } n = 0, \text{ so that } n + 1 = J(0, 1) \in Z.$$

Thus we have shown that $0 \in Z$, and that $n \in Z$ implies $n + 1 \in Z$, from which we infer $Z = \mathbb{N}_0$. \dashv

This construction permits us to construct an enumeration of the set of all non-empty sequences of elements of \mathbb{N}_0 . First we have a look at sequences of fixed length. For this, define inductively

$$\begin{aligned} \tau_1(x) &:= x, \\ \tau_{k+1}(x_1, \dots, x_k, x_{k+1}) &:= J(\tau_k(x_1, \dots, x_k), x_{k+1}) \end{aligned}$$

($x \in \mathbb{N}_0$ and $k \in \mathbb{N}$, $\langle x_1, \dots, x_{k+1} \rangle \in \mathbb{N}_0^{k+1}$), the idea being that an enumeration of $\mathbb{N}^k \times \mathbb{N}$ is reduced to an enumeration of $\mathbb{N} \times \mathbb{N}$, an enumeration of which in turn is known.

Proposition 1.4 *The maps τ_k are bijections $\mathbb{N}_0^k \rightarrow \mathbb{N}_0$.*

Proof 1. The proof proceeds by induction on k . It is trivial for $k = 0$. Now assume that we have established bijectivity for $\tau_k : \mathbb{N}_0^k \rightarrow \mathbb{N}_0$.

2. τ_{k+1} is injective: Assume $\tau_{k+1}(x_1, \dots, x_k, x_{k+1}) = \tau_{k+1}(x'_1, \dots, x'_k, x'_{k+1})$, this means

$$J(\tau_k(x_1, \dots, x_k), x_{k+1}) = J(\tau_k(x'_1, \dots, x'_k), x'_{k+1}),$$

hence $\tau_k(x_1, \dots, x_k) = \tau_k(x'_1, \dots, x'_k)$ and $x_{k+1} = x'_{k+1}$ by Proposition 1.3. By induction hypothesis, $\langle x_1, \dots, x_k \rangle = \langle x'_1, \dots, x'_k \rangle$.

3. τ_{k+1} is onto: Given $n \in \mathbb{N}_0$, there exists $\langle a, b \rangle \in \mathbb{N}_0 \times \mathbb{N}_0$ with $J(a, b) = n$. Given $a \in \mathbb{N}_0$, there exists $\langle x_1, \dots, x_k \rangle \in \mathbb{N}_0^k$ with $\tau_k(x_1, \dots, x_k) = a$ by induction hypothesis, so

$$n = J(a, b) = J(\tau_k(x_1, \dots, x_k), b) = \tau_{k+1}(x_1, \dots, x_k, b).$$

\dashv

From this, we can manufacture a bijection

$$\bigcup_{k \in \mathbb{N}} \mathbb{N}_0^k \rightarrow \mathbb{N}_0$$

in this way. Given a finite sequence v of natural numbers, we use its length, say, k , as one parameter of an enumeration of $\mathbb{N} \times \mathbb{N}$, the other parameter for this enumeration is $\tau_k(v)$. This yields a bijection.

Proposition 1.5 *There exists a bijection $\sigma : \bigcup_{k \in \mathbb{N}} \mathbb{N}_0^k \rightarrow \mathbb{N}_0$.*

Proof Define

$$\sigma(x_1, \dots, x_k) := J(k, \tau_k(x_1, \dots, x_k))$$

for $k \in \mathbb{N}$ and $\langle x_1, \dots, x_k \rangle \in \mathbb{N}_0^k$. Because J and τ_k both are injective, σ is injective. Given $n \in \mathbb{N}_0$, we can find $\langle a, b \rangle \in \mathbb{N}_0 \times \mathbb{N}_0$ with $J(a, b) = n$. Given $b \in \mathbb{N}_0$, we can find $\langle x_1, \dots, x_a \rangle \in \mathbb{N}_0^a$ with $\tau_a(x_1, \dots, x_a) = b$, so that

$$n = J(a, b) = J(a, \tau_a(x_1, \dots, x_a)).$$

Hence σ is also surjective. \dashv

One wonders why we did go through this somewhat elaborate construction. First, the construction is elegant in its simplicity, but there is another, more subtle reason. When tracing the arguments leading to Proposition 1.5 one sees that the argumentation is elementary, it does not require any set theoretic assumptions like (\mathbb{AC}) .

Proposition 1.6 *Let $\{A_n \mid n \in \mathbb{N}_0\}$ be a sequence of countably infinite sets. Then (\mathbb{AC}) implies that $\bigcup_{n \in \mathbb{N}_0} A_n$ is countable.*

Proof We assume for simplicity that the A_n are mutually disjoint. Given $n \in \mathbb{N}_0$ there exists an enumeration $\psi_n : A_n \rightarrow \mathbb{N}_0$. (\mathbb{AC}) permits us to fix for each n such an enumeration ψ_n , then define

$$\psi : \begin{cases} \bigcup_{n \in \mathbb{N}_0} A_n & \rightarrow \mathbb{N}_0 \\ x & \mapsto J(k, \psi_k(x)), \text{ if } x \in A_k \end{cases}$$

with J as the bijection defined in Proposition 1.3. \dashv

Having (\mathbb{AC}) , hence Proposition 1.6 at our disposal, one shows by induction that

$$\mathbb{N}_0^{k+1} = \bigcup_{n \in \mathbb{N}_0} \mathbb{N}_0^k \times \{n\}$$

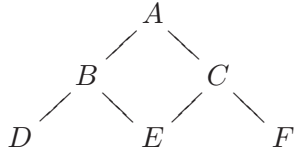
is countable for every $k \in \mathbb{N}$. This establishes the countability of $\bigcup_{k \in \mathbb{N}} \mathbb{N}_0^k$ immediately. On the other hand it can be shown that Proposition 1.6 is not valid if (\mathbb{AC}) is not assumed [KM76, p. 172] or [Her06, Section 3.1]. This is also true if (\mathbb{AC}) is weakened somewhat to postulate the existence of a choice function for *countable* families of non-empty sets (which in our case would suffice). The proof of non-validity, however, is in either case far beyond our scope.

1.3 Well-Ordered Sets

A relation R on a set M is called an *order relation* iff it is *reflexive* (thus xRx holds for all $x \in M$), *antisymmetric* (this means that xRy and yRx implies $x = y$ for all $x, y \in M$) and *transitive* (hence xRy and yRz implies xRz for all $x, y, z \in M$). The relation R is called *linear* iff one of the cases $x = y$, xRy or yRx applies for all $x, y \in M$, and it is called *relation!strict* strict iff xRx is false for each $x \in M$. If R is strict and transitive, then it is called a *strict order*.


Let R be an order relation then $x \in M$ is called a *lower bound* for $\emptyset \neq A \subseteq M$ iff xRz holds for all $z \in A$ and a *smallest element* for A iff it is both a lower bound for A and a member of A . *Upper bounds* and *largest elements* are defined similarly. An element y is called *maximal* iff there exists no element x with yRx , *minimal* elements are defined similarly. A *minimal upper bound* for a set $A \neq \emptyset$ is called the *supremum* of A and denoted by $\sup A$, similarly, a *maximal lower bound* for A is called the *infimum* of A and denoted by $\inf A$. Neither infimum nor supremum of a non-empty set need to exist.


Example 1.7 Look at this ordered set:



Here A is the maximum, because every element is smaller than A ; the minimal elements are D , E and F , but there is no minimum. The minimal elements cannot be compared to each other.



Example 1.8 Define $a \leq_d b$ iff a divides b for $a, b \in \mathbb{N}$, thus $a \leq_d b$ iff there exists $k \in \mathbb{N}$ such that $b = k \cdot a$. Let g be the greatest common divisor of a and b , then $g = \inf\{a, b\}$, and if s is the smallest common multiple of a and b , then $s = \sup\{a, b\}$. Here is why: One notes first that both $g \leq_d a$ and $g \leq_d b$ holds, because g is a common divisor of a and b . Let g' be another common divisor of a and b , then one shows easily that g' divides g , so that $g' \leq_d g$ holds. Thus g is in fact the greatest common divisor. One argues similarly for the lowest common multiple of a and b . 


Example 1.9 Order $S := \mathcal{P}(\mathbb{N}) \setminus \{\mathbb{N}\}$ by inclusion. Then $\mathbb{N} \setminus \{k\}$ is maximal in S for every $k \in \mathbb{N}$. For we obtain from the definition of S and its order that each element which contains $\mathbb{N} \setminus \{k\}$ properly would be outside the basic set S . The set $A := \{\{n, n+2\} \mid n \in \mathbb{N}\}$ is unbounded in S . Assume that T is an upper bound for A , then $n \in \{n, n+2\} \subseteq T$ and for each $n \in \mathbb{N}$, so that $T = \mathbb{N} \notin S$. 

Usually strict orders are written as $<$ (or $<_M$, if the basis set is to be emphasized), and order relations as \leq or \leq_M , resp.


Let $<_M$ be a strict order on M , $<_N$ be a strict order on N , then a map $f : M \rightarrow N$ is called *increasing* iff $x <_M y$ implies $f(x) <_N f(y)$; M and N are called *similar* iff f is a bijection such that $x <_M y$ is equivalent to $f(x) <_N f(y)$. An *order isomorphism* is a bijection which together with its inverse is increasing.

Definition 1.10 The strict linear order $<$ on a set M is called a *well-ordering* on M iff each non-empty subset of M has a smallest element. M is then called *well-ordered* (under $<$).

These are simple examples of well-ordered sets.

Example 1.11 \mathbb{N} (this shows the special rôle of \mathbb{N} alluded to above), finite linearly ordered sets, and $\{1 - \frac{1}{n} \mid n \in \mathbb{N}\}$ are well-ordered. 

Not every ordered set, however, is well-ordered, witnessed by these simple examples.

Example 1.12 \mathbb{Z} is not well-ordered, because it does not have a minimal element. \mathbb{R} is neither, because, e.g., the open interval $]0, 1[$ does not have a smallest element. The powerset of \mathbb{N} , denoted by $\mathcal{P}(\mathbb{N})$, is not well-ordered by inclusion because a well-order is linear, and $\{1, 2\}$ and $\{3, 4\}$ are not comparable. Finally, $\{1 + \frac{1}{n} \mid n \in \mathbb{N}\}$ is not well-ordered, because the set does not contain a smallest element. 

Example 1.13 A *reduction system* $\mathcal{R} = (A, \rightarrow)$ is a set A together with a relation $\rightarrow \subseteq A \times A$; the intent is to have a set of rewrite rules, say, $\langle a, b \rangle \in \rightarrow$ such that a may be replaced by b in words over an alphabet which includes the carrier A of \mathcal{R} . Usually, one writes $a \rightarrow b$ iff

$\langle a, b \rangle \in \rightarrow$. Denote by $\overset{+}{\rightarrow}$ the reflexive-transitive closure of relation \rightarrow , i.e., $x \overset{+}{\rightarrow} y$ iff $x = y$ or there exists a chain $x = a_0 \rightarrow \dots \rightarrow a_k = y$.

We call \mathcal{R} *terminating* iff there are no infinite chains $a_0 \rightarrow a_1 \rightarrow \dots \rightarrow a_k \rightarrow \dots$. The following proof rule is associated with a reduction system:

$$(WFI) \frac{\forall x \in A (\forall y \in A : x \overset{+}{\rightarrow} y \Rightarrow P(y)) \Rightarrow P(x)}{\forall x \in A : P(x)}$$

Here P is a predicate on A so that $P(x)$ is true iff x has property P . The rule (WFI) says that if we can conclude for every x that $P(x)$ holds, provided the property holds for all predecessors of x , then we may conclude that P holds for each element of A .

This rule is equivalent to termination. In fact

- If \rightarrow terminates, then (WFI) holds. Assume that (WFI) does not hold, then we find $x_0 \in A$ such that $P(x_0)$ does not hold, hence we can find some x_1 with $x_0 \overset{+}{\rightarrow} x_1$ and $P(x_1)$ does not hold. For x_1 we find x_2 for which P does not hold with $x_1 \overset{+}{\rightarrow} x_2$, etc. Hence we construct an infinite chain $x_0 \overset{+}{\rightarrow} x_1 \overset{+}{\rightarrow} \dots$ of elements for which P does not hold. But this means that \rightarrow does not terminate.
- If (WFI) holds, then \rightarrow terminates. Take the predicate $P(x)$ iff *there is not infinite chain starting from x* . Now (WFI) says that if $y \overset{+}{\rightarrow} x$, and if $P(y)$ holds, that then $P(x)$ holds. This means that no infinite chain starts from y , and x is a successor to y , that then no infinite chain starts from x either. Hence, by the conclusion of this rule, no x is the starting point of an infinite chain, consequently \rightarrow terminates.

Now let (A, \rightarrow) be a terminating reduction system, then each non-empty subset $B \subseteq A$ has a minimal element, because if this is not the case, we can construct an infinite descending chain. But (A, \rightarrow) is usually not well-ordered, because $\overset{+}{\rightarrow}$ is not necessarily strict. \mathbb{M}

There are some helpful ways of producing a new well-order from old ones.

Example 1.14 Let M and N be well-ordered and disjoint sets, define on $M \cup N$

$$a < b \text{ iff } \begin{cases} a <_M b, & \text{if } a, b \in M, \\ a <_N b, & \text{if } a, b \in N, \\ a \in M, b \in N, & \text{otherwise.} \end{cases}$$

Then $M \cup N$ is well-ordered; this well-ordered set is usually denoted by $M + N$. Note that $M + N$ is not the same as $N + M$. If the sets are not disjoint, make a copy of each upon setting $M' := M \times \{1\}$, $N' := N \times \{2\}$, and order these sets through, e.g. $\langle m, 1 \rangle <_{M'} \langle m', 1 \rangle$ iff $m <_M m'$. \mathbb{M}

Example 1.15 Define on the Cartesian product $M \times N$

$$\langle m, n \rangle < \langle m', n' \rangle \text{ iff } \begin{cases} m < m' \\ n < n', & \text{if } m = m' \end{cases}$$

This *lexicographic order* yields a well-ordering again. \mathbb{M}

Example 1.16 Let Z be well-ordered, and assume that for each $z \in Z$ the set M_z is well-ordered so that the sets $(M_z)_{z \in Z}$ are mutually disjoint. Then $\bigcup_{z \in Z} M_z$ is well-ordered. \mathfrak{M}

Having a look at $(\mathbb{A}\mathbb{C})$ again, we see that it holds in a well-ordered set:

Proposition 1.17 *Let \mathcal{F} be a family of non-empty subsets of the well-ordered set M . Then there exists a choice function on \mathcal{F} .*

Proof For each $F \in \mathcal{F}$ there exists a smallest element $m_F \in F$. Put $f(F) := m_F$, then $f : \mathcal{F} \rightarrow M$ is a choice function on \mathcal{F} . \dashv

Thus, if we can find a well-order on a set, then we know that we can find choice functions. We formulate first this property.

(WO) Each set can be well-ordered.

We will refer to this property as (WO). Hence we can rephrase Proposition 1.17 as

$$(\text{WO}) \implies (\mathbb{A}\mathbb{C})$$

Establishing the converse will turn out to be more interesting, since it will require the introduction of a new class of objects, viz., the ordinal numbers. This is what we will be doing next.

We start with some preparations which deal with properties of well-orders.

Lemma 1.18 *Let M be well-ordered and $f : M \rightarrow M$ be an increasing map. Then $x \leq_M f(x)$ (thus $x < f(x)$ or $x = f(x)$) holds for all $x \in M$.*

Proof Suppose that the set $Y := \{y \in M \mid f(y) < y\}$ is not empty, then it has a smallest element z . Since $f(z) < z$ we obtain $f(f(z)) < f(z) < z$, because f is increasing. This contradicts the choice of z . \dashv

Let M be well-ordered, then define for $x \in M$ the *initial segment* $O(x)$ (or $O_M(x)$) for x as $O(x) := \{z \in M \mid z < x\}$.

We obtain as a consequence

Corollary 1.19 *No well-ordered set is order isomorphic to an initial segment of itself.*

Proof An isomorphism $f : M \rightarrow O_M(x)$ for some $x \in M$ would have $f(x) < x$, which contradicts Lemma 1.18. \dashv

A surprising consequence of Lemma 1.18 is that there exists at most one isomorphism between well-ordered sets.

Corollary 1.20 *Let A and B be well-ordered sets. If $f : A \rightarrow B$ and $g : A \rightarrow B$ are order isomorphisms, then $f = g$.*

Proof Clearly both $g^{-1} \circ f$ and $f^{-1} \circ g$ are increasing, yielding $x \leq (g^{-1} \circ f)(x)$ and $x \leq (f^{-1} \circ g)(x)$ for each $x \in A$, which means $g(x) \leq f(x)$ and $f(x) \leq g(x)$ for each $x \in A$. \dashv

This is an important property of well-ordered sets akin to induction in the set of natural numbers. Accordingly it is called the *principle of transfinite induction*, sometimes also called *Noetherian induction* (after the eminent German mathematician Emmy Noether) or *well-founded induction* (after the virtual unknown Chinese mathematician Wēl Fūn Dèd).

Theorem 1.21 *Let M be well-ordered, $B \subseteq M$ be a set which has for each $x \in M$ the property that $O(x) \subseteq B$ implies $x \in B$. Then $B = M$.*

Proof Assume that $M \setminus B \neq \emptyset$, then there exists a smallest element x in this set. Since x is minimal, all elements smaller than x are elements of B , hence $O(x) \subseteq B$. But this implies $x \in B$, a contradiction. \dashv

Let us have a look at a proof of Lemma 1.18 using the principle of transfinite induction. Put $B := \{z \in M \mid z \leq f(z)\}$, and assume $O(x) \subseteq B$. If $y \in B$ with $y \neq f(y)$, then $y < f(y)$ and $y < x$, so that $f(y) < f(x)$, thus $y < f(x)$. Hence $f(x)$ is larger than any element of $O(x)$, thus $f(x) \in M \setminus O(x)$. But x is the smallest element of the latter set, which implies $x < f(x)$, so $x \in B$. From Theorem 1.21 we see now that $B = M$.

We will show now that each set can be well ordered. In order to do this, we construct a prototypical well order and show that each set can be mapped bijectively to this set. This then will serve as the basis for the construction of a well order for this set.

Carrying out this programme requires the prototype. This will be considered next.

1.4 Ordinal Numbers

Following von Neumann [KM76, § VII.9], ordinal numbers are defined as sets with these special properties.

Definition 1.22 *A set α is called an ordinal number iff these conditions are satisfied*

- ① *Every element of α is a set.*
- ② *If $\beta \in \alpha$, then $\beta \subseteq \alpha$.*
- ③ *If $\beta, \gamma \in \alpha$, then $\beta = \gamma$ or $\beta \in \gamma$ or $\gamma \in \beta$.*
- ④ *If $\emptyset \neq B \subseteq \alpha$, then there exists $\gamma \in B$ with $\gamma \cap B = \emptyset$.*

Hence in order to show that a given set is an ordinal, we have to show that the properties ①, ②, ③ and ④ hold. We will demonstrate this principle for some examples.

Example 1.23 Consider this definition of the *somewhat natural numbers* \mathfrak{N}_0

$$\begin{aligned} 0 &:= \emptyset, \\ n+1 &:= \{0, \dots, n\}, \\ \mathfrak{N}_0 &:= \{0, 1, \dots\}. \end{aligned}$$

Then \mathfrak{N}_0 is an ordinal number. Each element of \mathfrak{N}_0 is a set by definition. Let $\beta \in \mathfrak{N}_0$. If $\beta = 0$, $\beta = \emptyset \subseteq \mathfrak{N}_0$, if $\beta \neq 0$, $\beta = n = \{0, \dots, n-1\} \subseteq \mathfrak{N}_0$. One argues similarly for property ③. Finally, let $\emptyset \neq \beta \subseteq \mathfrak{N}_0$, and let γ be the smallest element of β . If $\delta \in \gamma \cap \beta$, then δ is both an element of β and smaller than γ , hence $\gamma \cap \delta = \emptyset$. \mathfrak{N}

Example 1.24 Let α be an ordinal number, then $\beta := \alpha \cup \{\alpha\}$ is an ordinal. It is the smallest ordinal which is greater than α . Property ① is evident, so is property ②. Let $\gamma, \gamma' \in \beta$ with $\gamma \neq \gamma'$, and assume that, say, $\gamma = \alpha$, then $\gamma' \neq \alpha$, consequently $\gamma' \in \gamma$. If neither γ nor γ' are equal to α , property ③ trivially holds. Assume finally that $\emptyset \neq B \subseteq \beta$. If $B \cap \alpha \neq \emptyset$, property ④ for β follows from this property for α , if, however, $B = \{\alpha\}$, observe that $\alpha \in \beta$ with $B \cap \alpha = \emptyset$. Hence this property holds for β as well. \mathbb{M}

Definition 1.25 Let α be an ordinal, then $\alpha \cup \{\alpha\}$ is called the successor to α and denoted by $\alpha + 1$.

It is clear from this definition that no ordinal can be squeezed in between an ordinal α and its successor $\alpha + 1$.

Lemma 1.26 If M is a non-empty set of ordinals, then

1. $\alpha_* := \bigcap M$ is an ordinal; it is the largest ordinal contained in all elements of M .
2. $\alpha^* := \bigcup M$ is an ordinal; it is the smallest ordinal which contains all elements of M .

Proof We iterate over the defining properties of an ordinal number for $\bigcap M$. Since every element γ of $\bigcap M$ is also an element of every $\alpha \in M$, we may conclude that γ is a set, and that $\gamma \subseteq \bigcap M$. If $\gamma, \delta \in \bigcap M \subseteq \alpha$ for each $\alpha \in M$, we have either $\gamma = \delta$, $\gamma \in \delta$ or $\delta \in \gamma$. Finally, if $\emptyset \neq B \subseteq \bigcap M \subseteq \alpha$ for each $\alpha \in M$, we find $\eta \in B$ such that $\eta \cap B = \emptyset$. Thus $\alpha_* := \bigcap M$ has all the properties of an ordinal number from Definition 1.22. It is clear that α_* is the largest ordinal contained in all elements of M .

The proof for $\bigcup M$ works along the same lines. \dashv

Corollary 1.27 Given a non-empty set M of ordinals, there is always an ordinal which is strictly larger than all the elements of M .

Proof If $\alpha^* := \bigcup M \in M$, then $\alpha^* + 1$ is the desired ordinal, otherwise α^* is suitable. \dashv

This is an interesting consequence.

Corollary 1.28 There is no set of all ordinals.

Proof If Z is the set of all ordinals, then Lemma 1.26 shows that $\alpha^* := \bigcup Z$ is an ordinal. But the successor $\alpha^* + 1$ to α^* is an ordinal as well by Example 1.24, which, however, is not an element of Z . This is a contradiction. \dashv

Definition 1.29 An ordinal λ is called a limit ordinal iff $\alpha < \lambda$ implies $\alpha + 1 < \lambda$ for all ordinals α .

Thus a limit ordinal is not reachable through the successor operation. This is a convenient characterization of limit ordinals.

Proposition 1.30 Let λ be an ordinal. Then

1. If λ is a limit ordinal, then $\bigcup \lambda = \lambda$.
2. If $\bigcup \lambda = \lambda$, then λ is a limit ordinal.

Proof 1. Let $\beta \in \bigcup \lambda$, then $\beta \in \alpha$ for some $\alpha \in \lambda$. Since α is an ordinal, we conclude $\beta \in \alpha \subseteq \lambda$, so $\bigcup \lambda \subseteq \lambda$. On the other hand, if $\alpha \in \lambda$, then $\alpha + 1 \in \lambda$, since λ is a limit ordinal. Thus $\alpha \in \bigcup \lambda$, so $\bigcup \lambda \supseteq \lambda$. This proves part 1.

2. Let $\alpha < \lambda = \bigcup \lambda$, then $\alpha \in \beta$ for some $\beta \in \lambda$. Then either $\alpha + 1 \in \beta$ or $\alpha + 1 = \beta$, in any case $\alpha + 1 \subseteq \beta$, so that $\alpha + 1 \in \lambda$. Thus λ is a limit ordinal. This establishes part 2. \dashv

Ordinals can be *odd* or *even*: A limit ordinal is said to be even; if the ordinal ζ can be written as $\zeta = \xi + 1$ and ξ is even, then ζ is odd, if ξ is odd, ζ is even. This classification is sometimes helpful, some constructions involving ordinals depend on it, see for example Section 1.6.1 on page 47.

Several properties of ordinal numbers are established now; this is required for carrying out the programme sketched above. The first property states that the \in -relation is not cyclic, which seems to be trivial. But since ordinal numbers have the dual face of being elements and subsets of the same set, we will need to exclude this property explicitly by showing that the properties of ordinals prevent this undesired behavior.

Lemma 1.31 *If α is an ordinal number, then there does not exist a sequence β_1, \dots, β_k of sets with $\beta_k \in \beta_1 \in \dots \beta_{k-1} \in \beta_k \in \alpha$.*

Proof If there exists such sets β_1, \dots, β_k , put $\gamma := \{\beta_1, \dots, \beta_k\}$. Now $\beta_k \in \alpha$ implies $\beta_k \subseteq \alpha$, thus $\beta_{k-1} \in \alpha$, hence $\beta_{k-1} \subseteq \alpha$, so that $\beta_1, \dots, \beta_k \in \alpha$. But now $\beta_{i-1} \in \beta_i \cap \gamma$ for $1 \leq i \leq k$ and $\beta_k \in \beta_1 \cap \gamma$, so that property ④ in Definition 1.22 is violated. \dashv

Lemma 1.32 *If α is an ordinal, then each $\beta \in \alpha$ is an ordinal as well.*

Proof 1. The properties of ordinal numbers from Definition 1.22 are inherited. This is immediate for properties ①, ③ and ④, so we have to take care of property ②.

2. Let $\gamma \in \beta$, we have to show that $\gamma \subseteq \beta$. So if $\eta \in \gamma$, we have by property ③ for α in the definition of ordinals either $\eta = \gamma$ (which would imply $\gamma \in \gamma \in \beta \in \alpha$, contradicting Lemma 1.31), or $\gamma \in \eta$ (which would yield $\gamma \in \eta \in \gamma \in \beta \in \alpha$, contradicting Lemma 1.31 again). Thus $\eta \in \beta$, so that property ② also holds. \dashv

Lemma 1.33 *Let α and β be ordinals, then these properties are equivalent*

1. $\alpha \in \beta$.
2. $\alpha \subseteq \beta$ and $\alpha \neq \beta$.

Proof 1 \Rightarrow 2: We obtain $\alpha \subseteq \beta$ from $\alpha \in \beta$ and from property ②, and $\alpha \neq \beta$ from Lemma 1.31, for otherwise we could conclude $\beta \in \beta$.

2 \Rightarrow 1: Because α is a proper subset of β , thus $\emptyset \neq \beta \setminus \alpha \subseteq \beta$, we infer from property ④ for ordinals that we can find $\gamma \in \beta \setminus \alpha$ such that $\gamma \cap \beta \setminus \alpha = \emptyset$. We claim that $\gamma = \alpha$.

“ \subseteq ”: Since $\gamma \in \beta$ we know that $\gamma \subseteq \beta$, and since $\gamma \cap \beta \setminus \alpha = \emptyset$, it follows $\gamma \subseteq \alpha$.

“ \supseteq ”: We will show that the assumption $\alpha \setminus \gamma \neq \emptyset$ is contradictory. Because $\emptyset \neq \alpha \setminus \gamma \subseteq \alpha$ we find $\eta \in \alpha \setminus \gamma$ with $\eta \cap \alpha \setminus \gamma = \emptyset$. Because $\eta \in \alpha \setminus \gamma \subseteq \alpha \subseteq \beta$ we conclude $\eta \in \beta$. From property ③ we infer that the cases $\eta = \gamma$, $\eta \in \gamma$ and $\gamma \in \eta$ may occur. Let us discuss look at these cases in turn

- $\eta = \gamma$: This is impossible, because we would have then $\eta \in \alpha$ and $\eta \in \beta \setminus \alpha$.

- $\eta \in \gamma$: This is impossible because $\eta \in \alpha \setminus \gamma$.
- $\gamma \in \eta$: We know that $\gamma \notin \alpha \setminus \gamma$, but $\gamma \in \alpha$, which implies $\gamma \in \gamma \in \alpha$, contradicting Lemma 1.31.

Thus we conclude that the assumption $\alpha \setminus \gamma \neq \emptyset$ leads us to a contradiction, from which the desired inclusion is inferred.

⊥

Consequently, the containment relation \in yields a total order on an ordinal number.

Lemma 1.34 *If α and β are ordinals, then either $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$.*

Proof Suppose $\alpha \neq \alpha \cap \beta \neq \beta$, then $\alpha \cap \beta \in \alpha$ and $\alpha \cap \beta \in \beta$ by Lemma 1.33, hence $\alpha \cap \beta \in \alpha \cap \beta$, contradicting Lemma 1.31. ⊥

Lemma 1.35 *Every ordinal is well-ordered by the inclusion relation.*

Proof Let α be an ordinal, we show first that α is linearly ordered by inclusion. Take $\beta, \gamma \in \alpha$, then either $\beta = \gamma$, $\beta \in \gamma$ or $\gamma \in \beta$. The last two conditions translate because of property ② to $\beta \subseteq \gamma$ or $\gamma \subseteq \beta$. Now let B be a non-empty subset of α , then we know from property ④ that there exists $\gamma \in B$ with $\gamma \cap B = \emptyset$. This is the smallest element of B . In fact, let $\eta \in B$ with $\eta \neq \gamma$, then either $\gamma \in \eta$ or $\eta \in \gamma$. But $\gamma \in \eta$ is impossible, since otherwise $\gamma \in B \cap \eta$. So $\eta \in \gamma$, hence $\eta \subseteq \gamma$. ⊥

We can describe this strict order even a bit more precise.

Lemma 1.36 *If α and β are distinct ordinals, then either α is an initial segment of β or β is an initial segment of α .*

Proof Because $\alpha \neq \beta$, we have either $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$ by Lemma 1.34. Assume that $\alpha \subseteq \beta$ holds. If $\gamma \in \alpha$, then $\gamma \subseteq \alpha$, thus all elements of α precede the element α ; conversely, if $\eta \in \beta$ with $\eta \subseteq \alpha$, then $\eta \in \alpha$. Hence α is a segment of β . It cannot be similar to β because of Corollary 1.19. ⊥

Historically, ordinal numbers have been introduced as some sort of equivalence classes of well-ordered sets under order isomorphisms (note that *some sort of equivalence classes* is a cautionary expression, alluding to the fact that there is no such thing as a set of all sets). We show now that the definition given here is not too far away from the traditional definition. Loosely speaking, the ordinals defined here may serve as representatives for those classes of well-ordered sets. We want to establish

Theorem 1.37 *If M is a well-ordered set, then there exists an ordinal α such that M and α are isomorphic.*

The proof will be done in several steps. Call two well-ordered sets A and B *similar* ($A \sim B$) iff there exists an isomorphism between them. Recall that isomorphisms preserve order relations in both directions.

Define the set H as all elements of M the initial segment of which is similar to some ordinal number, i.e.,

$$H := \{z \in M \mid \alpha_z \sim O(z) \text{ for some ordinal } \alpha_z\}.$$

In view of Lemma 1.36, if $\alpha_z \sim O(z)$ and $\alpha'_z \sim O(z)$, then $\alpha_z = \alpha'_z$, so the ordinal α_z is uniquely determined, if it exists. We first show by induction that $H = M$. For this, assume that $O(z) \subseteq H$, then we have to show that $z \in H$, so we have to find an ordinal α_z with $\alpha_z \sim O(z)$. In fact, the natural choice is

$$\alpha_z := \{\alpha_x \in M \mid x < z\},$$

so we show that this is an ordinal number by going through the properties according to Definition 1.22. Since each element of α_z is an ordinal, property ① is satisfied. Let $\alpha_x \in \alpha_z$, then $x < z$; if $\eta \in \alpha_x$, then η is an ordinal number, hence an initial segment of α_x by Lemma 1.36, thus $\eta \sim O(t)$ for some t . Hence $t < x < z$, so that $\alpha_t = \eta \in \alpha_z$. Thus property ② is satisfied. Property ③ follows from Lemma 1.34: Take $\alpha_x, \alpha_y \in \alpha_z$, then α_x and α_y are ordinals. Assume that they are different, then either $\alpha_x \subseteq \alpha_y$ or $\alpha_y \subseteq \alpha_x$, so that by Lemma 1.33 $\alpha_x \in \alpha_y$ or $\alpha_y \in \alpha_x$ follows. Finally, let $\emptyset \neq B \subseteq \alpha_x$. Then B corresponds to a non-empty subset of M with a smallest element y . Then $\alpha_y \in \alpha_z$, because $y < z$, and we claim that $\alpha_y \cap B = \emptyset$. In fact, if $\eta \in \alpha_y \cap B$, then $\eta = \alpha_t$ for some $t \in B$, so that y would not be minimal. This shows that Property ④ is satisfied. Hence α_z is an ordinal. In order to establish that $z \in H$ we have to show that α_z is similar to $O(z)$. But this follows from the construction.

Consequently we know that the initial segment for each element of M is similar to an ordinal.

We are now in a position to complete the proof

Proof (for Theorem 1.37) Let

$$\alpha := \{\alpha_z \mid \alpha_z \sim O(z) \text{ for some } z \in M\},$$

then one shows with exactly the arguments from above that α is an ordinal. Moreover, α is similar to M : Consider the map $z \mapsto \alpha_z$, provided $\alpha_z \sim O(z)$. It is clear that it is one to one, since $x < y$ implies $\alpha_x \in \alpha_y$, for $O(x)$ is a (proper) initial segment of $O(y)$. It is also onto, because given $\eta \in \alpha$, we find $z \in M$ with $\eta \sim O(z)$, so that $z \mapsto \eta$. \dashv

Let us have a brief look at all countable ordinals. They will be used later on for a particular construction in Section 1.7 for the construction of a game, and in Section 1.6.1 for the construction of a σ -algebra.

Proposition 1.38 *Let $\omega_1 := \{\alpha \mid \alpha \text{ is a countable ordinal}\}$. Then ω_1 is an ordinal.*

Proof Exercise 11; the proof will have to look at the properties ① through ④. \dashv

Denote by $W(\alpha) := \{\zeta \mid \zeta < \alpha\}$ all ordinals smaller than α , hence the initial segment of ordinals determined by α . Given an arbitrary non-empty set S , a map $f : W(\alpha) \rightarrow S$ is called an α -sequence over S and sometimes denoted by $\langle a_\zeta \mid \zeta < \alpha \rangle$, where $a_\zeta := f(\zeta)$. The next very general statement says that these sequences can be defined by transfinite recursion in the following manner.

Theorem 1.39 *Let S be a non-empty set, and let Φ be the set of all α -sequences over S for some ordinal α . Moreover, assume that $h : \Phi \rightarrow S$ is a map of α -sequences over S to S . Then there exists a uniquely determined $(\alpha + 1)$ -sequence $\langle a_\zeta \mid \zeta \leq \alpha \rangle$ such that*

$$a_\zeta = h(\langle a_\xi \mid \xi < \zeta \rangle) \tag{1}$$

for all $\zeta \leq \alpha$.

Proof 1. We show uniqueness first. Assume that we have two $\alpha + 1$ -sequences $\langle a_\zeta \mid \zeta \leq \alpha \rangle$ and $\langle b_\zeta \mid \zeta \leq \alpha \rangle$ such that

$$\begin{aligned} a_\zeta &= h(\langle a_\eta \mid \eta < \zeta \rangle) \\ b_\zeta &= h(\langle b_\eta \mid \eta < \zeta \rangle) \end{aligned}$$

for all $\zeta \leq \alpha$. Then we show by induction on ζ that $a_\zeta = b_\zeta$. The induction begins at the smallest ordinal $\zeta = \emptyset$, so that $a_\emptyset = h(\emptyset) = b_\emptyset$, and the induction step is trivial.

2. The sequence $\langle a_\zeta \mid \zeta \leq \alpha \rangle$ is defined now by induction on ζ . If $\langle a_\eta \mid \eta \leq \zeta \rangle$ is defined, then define

$$\alpha_{\zeta+1} := h(\langle a_\eta \mid \eta \leq \zeta \rangle).$$

If, however, λ is a limit ordinal such that $\langle a_\eta \mid \eta \leq \zeta \rangle$ is defined for each $\zeta < \lambda$, then one notes that $\langle a_\xi \mid \xi < \zeta' \rangle$ is the restriction of $\langle a_\xi \mid \xi < \zeta \rangle$ for $\zeta < \zeta' < \lambda$ by uniqueness, so that

$$\alpha_\lambda := h(\langle a_\zeta \mid \zeta < \lambda \rangle)$$

defines α_λ uniquely. \dashv

We are now in a position to show that the existence of a choice function implies that each set S can be well-ordered. The idea of the proof is to find for some suitable ordinal α an α -sequence $\langle a_\zeta \mid \zeta < \alpha \rangle$ over S which exhausts S , hence so that $S = \{a_\zeta \mid \zeta < \alpha\}$, and then to use the well-ordering of the ordinals by saying that $a_\zeta < a_\xi$ iff $\zeta < \xi$.

Constructing the sequence will use the choice function, selecting an element in such a way that one can be sure that it has not been selected previously.

Theorem 1.40 *If (\mathbb{AC}) holds, then each set S can be well-ordered.*

Proof Let $f : \mathcal{P}(S) \setminus \{\emptyset\} \rightarrow S$ be a choice function on the non-empty subset of S . Extend f by putting $f(\emptyset) := p$, where $p \notin S$. This element p serves as an indicator that we are done with constructing the sequence. Let \mathcal{C} be the set of all ordinals ζ such that there exists a well-order $<_B$ on a subset $B \subseteq S$ with $(B, <_B) \sim O(\zeta)$ (cp. Theorem 1.37). Since \mathcal{C} is a set of ordinals, there exists a smallest ordinal α not in \mathcal{C} by Corollary 1.27.

By Theorem 1.39 there exists an α -sequence $\langle a_\zeta \mid \zeta < \alpha \rangle$ over S such that $a_\zeta := f(S \setminus \langle a_\eta \mid \eta < \zeta \rangle) \in S \setminus \langle a_\eta \mid \eta < \zeta \rangle$ for all $\zeta < \alpha$. Now if $S \setminus \langle a_\eta \mid \eta < \zeta \rangle \neq \emptyset$, then $a_\zeta \neq p$, and $a_\zeta \notin \langle a_\eta \mid \eta < \zeta \rangle$, so that the a_ζ are mutually different. Suppose that this process does not exhaust S , then $a_\zeta \neq p$ for all $\zeta < \alpha$. Construct the corresponding well-order $<$ on $\{a_\zeta \mid \zeta < \alpha\}$, then $(\{a_\zeta \mid \zeta < \alpha\}, <) \sim O(\alpha)$. Thus $\alpha \in \mathcal{C}$, contradicting the choice of α . Hence there exists a smallest ordinal $\xi < \alpha$ with $a_\xi = p$, which implies that $S = \{a_\zeta \mid \zeta < \xi\}$ so that elements having different labels are in fact different. This yields a well-order on S . \dashv

Hence we have shown

Theorem 1.41 *The following statements are equivalent*

(\mathbb{AC}) *The Axiom of Choice.*

(WO) *Each set can be well-ordered.*

⊥

(AC) has other important and often used equivalent formulations, which we will discuss now.

1.5 Zorn's Lemma and Tuckey's Maximality Principle

Let A be an ordered set, then $B \subseteq A$ is called a *chain* iff it is linearly ordered. Then Zorn's Lemma states

(ZL) If A is an ordered set in which every chain has an upper bound, then A has a maximal element.

Proposition 1.42 (ZL) *implies* (AC).

Proof Let $\mathcal{F} \neq \emptyset$ be a family of nonempty subsets of a set S , we want to find a choice function on \mathcal{F} . Define

$$R := \{\langle F, s \rangle \mid s \in F \in \mathcal{F}\},$$

then $R \subseteq \mathcal{F} \times S$ is a relation. Put

$$\mathcal{C} := \{f \mid f \text{ is a function with } f \subseteq R\}$$

(note that we use functions here as sets of pairs). Then $\mathcal{C} \neq \emptyset$, because $\langle F, s \rangle \in \mathcal{C}$ for each $\langle F, s \rangle \in R$. \mathcal{C} is ordered by inclusion, and each chain has an upper bound in \mathcal{C} . In fact, if $K \subseteq \mathcal{C}$ is a chain, then $\bigcup K$ is a map: let $\langle F, s \rangle, \langle F, s' \rangle \in \bigcup K$, then there exists $f_1, f_2 \in K$ with $\langle F, s \rangle \in f_1, \langle F, s' \rangle \in f_2$. Because K is a chain, either $f_1 \subseteq f_2$ or vice versa, let us assume $f_1 \subseteq f_2$. Thus $\langle F, s \rangle \in f_2$, and since f_2 is a map, we may conclude that $s = s'$. Hence $\bigcup K$ is an upper bound to K in \mathcal{C} .

By (ZL), \mathcal{C} has a maximal element f^* . We prove that f^* is the desired choice function, hence that there exists for each and every $F \in \mathcal{F}$ some $s \in F$ with $f^*(F) = s$, or, equivalently, $\langle F, s \rangle \in f^*$. Hence the domain of f^* should be all of \mathcal{F} . Assume that the domain of f^* does not contain some $F^* \in \mathcal{F}$, then the map $f^* \cup \{\langle F^*, a \rangle\}$ contains for each $a \in F^*$ the map f^* properly. This is a contradiction. Hence $f^* : \mathcal{F} \rightarrow S$ with $f^*(F) \in F$ for all $F \in \mathcal{F}$. ⊥

A proof for the other direction uses a well-ordering argument for constructing a maximal chain.

Proposition 1.43 *Assume that A is an ordered set in which each chain has an upper bound, and assume that there exists a choice function on $\mathcal{P}(A) \setminus \{\emptyset\}$. Then A has a maximal element.*

Proof 1. As in the proof of Theorem 1.40, let \mathcal{C} be the set of all ordinals ζ such that there exists a well-order $<_B$ on a subset $B \subseteq A$ with $(B, <_B) \sim O(\zeta)$, and let α be the smallest ordinal not in \mathcal{C} , see Corollary 1.27. Extend the choice function f on $\mathcal{P}(A) \setminus \{\emptyset\}$ upon setting $f(\emptyset) := p$ with $p \notin A$. This element will again serve as a marker, indicating that the selection process is finished.

2. Define by induction a transfinite sequence $\langle a_\zeta \mid \zeta < \alpha \rangle$ such that $a_\emptyset \in A$ is arbitrary and

$$a_\zeta := f(\{x \in A \mid x > a_\eta \text{ for all } \eta < \zeta\}).$$

Assume that $a_\zeta \neq p$, then $a_\zeta > a_\eta$ for all $\eta < \zeta$. As in the proof of Theorem 1.40, there is a smallest ordinal $\beta < \alpha$ such that $a_\beta = p$. The selection process makes sure that $\langle a_\zeta \mid \zeta < \beta \rangle$ is an increasing sequence, and that there does not exist an element $x \in A$ such that $a_\zeta < x$ for all $\zeta < \beta$.

3. Let t be an upper bound for the chain $\langle a_\zeta \mid \zeta < \beta \rangle$. If t is not a maximal element for A , then there exists x with $x > t$, hence $x > a_\zeta$ for all $\zeta < \beta$, which is a contradiction. \dashv

Call a subset $\mathcal{F} \subseteq \mathcal{P}(A)$ of *finite character* iff the following condition holds: F is a member of \mathcal{F} iff each finite subset of F is a member of \mathcal{F} . The following statement is known as *Tuckey's Lemma* or as *Tuckey's Maximality Principle*:

(MP) Each family of finite character has a maximal element.

This is another equivalent to (AC).

Proposition 1.44 (MP) \Leftrightarrow (AC).

Proof 0. We show (MP) \Rightarrow (AC), the other direction is delegated to the Exercises.

1. Let $\mathcal{F} \subseteq \mathcal{P}(S) \setminus \{\emptyset\}$ be a family of nonempty sets. We construct a choice function for \mathcal{F} . Consider

$$\mathcal{G} := \{f \mid f \text{ is a choice function for some } \mathcal{E} \subseteq \mathcal{F}\}.$$

Then \mathcal{G} is of finite character. In fact, let f be map from $\mathcal{E} \subseteq \mathcal{F}$ to S such that each finite subset $f_0 \subseteq f$ is a choice function for some $\mathcal{E}_0 \subseteq \mathcal{E}$, then f is itself a choice function for \mathcal{E} . Conversely, if $f : \mathcal{E} \rightarrow S$ is a choice function for $\mathcal{E} \subseteq \mathcal{F}$, then each finite subset of f is a choice function for its domain. Thus there exists by the Maximality Principle a maximal element $f^* \in \mathcal{G}$. The domain of f^* is all of \mathcal{F} , because otherwise f^* could be extended as in the proof of Proposition 1.42, and it is clear that f^* is a choice function on \mathcal{F} . \dashv

Thus we have shown

Theorem 1.45 *The following statements are equivalent*

(AC) *The Axiom of Choice.*

(WO) *Each set can be well-ordered.*

(ZL) *If A is an ordered set in which every chain has an upper bound, then A has a maximal element (Zorn's Lemma).*

(MP) *Each family of finite character has a maximal element (Tuckey's Maximality Principle).*

We will discuss some applications of Zorn's Lemma and the Maximality Principle now; from Theorem 1.45 we know that in each case we could use also (AC) or (WO), but an application of Zorn's Lemma appears to be more convenient and less technical.

1.5.1 Compactness for Propositional Logic

We will show that a set of propositional formulas is satisfiable iff each finite subset is satisfiable. This is usually called the Compactness Theorem for Propositional Logic.

Fix a set $V \neq \emptyset$ of variables. A propositional formula φ is given through this grammar

$$\varphi ::= x \mid \varphi \wedge \varphi \mid \neg \varphi$$

with $x \in V$. Hence a formula is either a variable, the conjunction of two formulas, or the negation of a formula. The disjunction $\varphi \vee \psi$ is defined through $\neg(\neg\varphi \wedge \neg\psi)$, implication $\varphi \rightarrow \psi$ as $\neg\varphi \vee \psi$, finally $\varphi \leftrightarrow \psi$ is defined through $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$. Denote by \mathcal{F} the set of all *propositional formulas* — actually, the set of all formulas depends on the set of variables, so we ought to write $\mathcal{F}(V)$; since we fix V , however, we use this somewhat lighter notation.

A *valuation* v evaluates formulas. Instead of using **true** and **false**, we use the values 0 and 1, hence a valuation is a map $V \rightarrow \{0, 1\}$ which is extended in a straightforward manner to a map $\mathcal{F} \rightarrow \{0, 1\}$, which is again denoted by v :

$$\begin{aligned} v(\varphi_1 \wedge \varphi_2) &:= \min\{v(\varphi_1), v(\varphi_2)\}, \\ v(\neg\varphi) &:= 1 - v(\varphi). \end{aligned}$$

Then we have obviously, e.g.,

$$\begin{aligned} v(\varphi_1 \vee \varphi_2) &= \max\{v(\varphi_1), v(\varphi_2)\}, \\ v(\varphi_1 \rightarrow \varphi_2) &= 1 \text{ iff } v(\varphi_1) \leq v(\varphi_2), \\ v(\varphi_1 \leftrightarrow \varphi_2) &= 1 \text{ iff } v(\varphi_1) = v(\varphi_2). \end{aligned}$$

For example,

$$\begin{aligned} v(\varphi \rightarrow (\psi \rightarrow \gamma)) &= \max\{1 - v(\varphi), \max\{1 - v(\psi), v(\gamma)\}\} \\ &= \max\{1 - v(\varphi), 1 - v(\psi), v(\gamma)\} \\ &= \max\{1 - v(\psi), \max\{1 - v(\varphi), v(\gamma)\}\} \\ &= v(\psi \rightarrow (\varphi \rightarrow \gamma)). \end{aligned}$$

Hence

$$\begin{aligned} (\varphi \rightarrow (\psi \rightarrow \gamma)) &\leftrightarrow (\psi \rightarrow (\varphi \rightarrow \gamma)) \\ &\leftrightarrow (\varphi \wedge \psi) \rightarrow \gamma. \end{aligned}$$

A formula is true for a valuation iff this valuation gives it the value 1; a set \mathcal{A} of formulas is satisfied by a valuation iff each formula in \mathcal{A} is true under this valuation. Formally:

Definition 1.46 *Let $v : \mathcal{F} \rightarrow \{0, 1\}$ be a valuation. Then formula φ is true for v (in symbols: $v \models \varphi$) iff $v(\varphi) = 1$. If $\mathcal{A} \subseteq \mathcal{F}$ is a set of propositional formulas, then \mathcal{A} is said to be satisfied by v iff each formula in \mathcal{A} is true for v , i.e., iff $v \models \varphi$ for all $\varphi \in \mathcal{A}$. This is written as $v \models \mathcal{A}$.*

We are interested in the question whether or not we can find for a set of formulas a valuation satisfying it.

Definition 1.47 $\mathcal{A} \subseteq \mathcal{F}$ is called *satisfiable* iff there exists a valuation $v : \mathcal{F} \rightarrow \{0, 1\}$ with $v \models \mathcal{A}$.

Depending on the size of the set of variables, the set of formulas may be quite large. If V is countable, however, \mathcal{F} is countable as well, so in this case the question may be easier to answer; this will be discussed briefly after giving the proof of the Compactness Theorem. We want to establish the general case.

Before we state and prove the result, we need a lemma which permits us to extend the range of our knowledge of satisfiability just by one formula.

Lemma 1.48 Let $\mathcal{A} \subseteq \mathcal{F}$ be satisfiable, and $\varphi \notin \mathcal{A}$ be a formula. Then one of $\mathcal{A} \cup \{\varphi\}$ and $\mathcal{A} \cup \{\neg\varphi\}$ is satisfiable.

Proof If $\mathcal{A} \cup \{\varphi\}$ is not satisfiable, but \mathcal{A} is, let v be the valuation for which $v \models \mathcal{A}$ holds. Because $v(\varphi) = 0$ we conclude $v(\neg\varphi) = 1$, so that $v \models \mathcal{A} \cup \{\neg\varphi\}$. \dashv

We establish now the *Compactness Theorem* for propositional logic. It permits reducing the question of satisfiability of a set \mathcal{A} of formulas to finite subsets of \mathcal{A} .

Theorem 1.49 Let $\mathcal{A} \subseteq \mathcal{F}$ be a set of propositional formulas. Then \mathcal{A} is satisfiable iff each finite subset of \mathcal{A} is satisfiable.

Proof We will focus on satisfiability of \mathcal{A} provided each finite subset of \mathcal{A} is satisfiable, because the other half of the assertion is trivial.

Let

$$\mathcal{C} := \{\langle \mathcal{B}, v \rangle \mid \mathcal{B} \subseteq \mathcal{A}, v \models \mathcal{B}\}$$

and define $\langle \mathcal{B}_1, v_1 \rangle \leq \langle \mathcal{B}_2, v_2 \rangle$ iff $\mathcal{B}_1 \subseteq \mathcal{B}_2$ and $v_1(\varphi) = v_2(\varphi)$ for all $\varphi \in \mathcal{B}_1$, so that $\langle \mathcal{B}_1, v_1 \rangle \leq \langle \mathcal{B}_2, v_2 \rangle$ holds iff \mathcal{B}_1 is contained in \mathcal{B}_2 , and if the valuations coincide on the smaller set. This is a partial order. If $\mathcal{D} \subseteq \mathcal{C}$ is a chain, then put $\mathcal{B} := \bigcup \mathcal{D}$, and define $v(\varphi) := v'(\varphi)$, if $\varphi \in \mathcal{B}'$ with $\langle \mathcal{B}', v' \rangle \in \mathcal{D}$. Since \mathcal{D} is a chain, v is well defined. Moreover, $v \models \mathcal{B}$: let $\varphi \in \mathcal{B}$, then $\varphi \in \mathcal{B}'$ for some $\langle \mathcal{B}', v' \rangle \in \mathcal{D}$, since $v' \models \mathcal{B}'$, we have $v(\varphi) = v'(\varphi) = 1$. Hence by Zorn's Lemma there exists a maximal element $\langle \mathcal{M}, w \rangle$, in particular $w \models \mathcal{M}$.

We claim that $\mathcal{M} = \mathcal{A}$. Suppose this is not the case, then there exists $\varphi \in \mathcal{A}$ with $\varphi \notin \mathcal{M}$. But either $\mathcal{M} \cup \{\varphi\}$ or $\mathcal{M} \cup \{\neg\varphi\}$ is satisfiable by Lemma 1.48, hence $\langle \mathcal{M}, w \rangle$ is not maximal. This is a contradiction.

But this means that $\mathcal{M} = \mathcal{A}$, hence \mathcal{A} is satisfiable. \dashv

Suppose that V is countable, then we know that \mathcal{F} is countable as well. Then another proof for Theorem 1.49 can be given; this will be sketched now. Enumerate \mathcal{F} as $\{\varphi_1, \varphi_2, \dots\}$. Call — just temporarily — $\mathcal{A} \subseteq \mathcal{F}$ *finitely satisfiable* iff each finite subset of \mathcal{A} is satisfiable. Let \mathcal{A} be such a finitely satisfiable set. We construct a sequence $\mathcal{M}_0, \mathcal{M}_1, \dots$ of finitely satisfiable sets, starting from $\mathcal{M}_0 := \mathcal{A}$. If \mathcal{M}_n is defined, put

$$\mathcal{M}_{n+1} := \begin{cases} \mathcal{M}_n \cup \{\varphi_{n+1}\} & \text{if } \mathcal{M}_n \cup \{\varphi_{n+1}\} \text{ is finitely satisfiable,} \\ \mathcal{M}_n \cup \{\neg\varphi_{n+1}\} & \text{otherwise.} \end{cases}$$

This will give a finitely satisfiable set $\mathcal{M}^* := \bigcup_{n \geq 0} \mathcal{M}_n$. Now define $v^*(\varphi) := 1$ iff $\varphi \in \mathcal{M}^*$. We claim that $v^* \models \varphi$ iff $\varphi \in \mathcal{M}^*$. This is proved by a straightforward induction on φ .

Because $\mathcal{A} \subseteq \mathcal{M}^*$, we know that $v^* \models \mathcal{A}$. This could be modified for the general case, well-ordering \mathcal{F} .

The approach used for the general proof can be extended from propositional logic to first-order logic by introducing suitable constants (they are called *Henkin constants*). We refer the reader to [Bar77, Chapter 1], since we are concentrating in the present text on applications of Zorn's Lemma.

1.5.2 Extending Orders

We will establish a generalization to the well-known fact that each finite graph \mathcal{G} can be embedded into a linear order, provided the graph does not have any cycles. This is known as a *topological sort* of the graph [Knu73, Algorithm T, p. 262] or [CLR92, Section 23.4]. One notes first that \mathcal{G} must have a node k which does not have any predecessor (hence there is no node ℓ which is connected to k with an edge $\ell \rightarrow k$). If such a node k would not exist, one could construct for each node a cycle on which it lies. The algorithm proceeds recursively. If the graph contains at most one node, it returns either the empty list or the list containing the node. The general case constructs a list having k as its head and the list for $\mathcal{G} \setminus k$ as its tail; here $\mathcal{G} \setminus k$ is the graph with node k and all edges emanating from k removed.

Finiteness plays a special rôle in the argument above, because it makes sure that we have a well-order among the nodes, which in turn is needed for making sure that the algorithm terminates. Let us turn to the general case. Given a partial order \leq on a set S , we show that \leq can be extended to a strict order \leq_s (hence $a \leq b$ implies $a \leq_s b$ for all $a, b \in S$).

This will be shown through Zorn's Lemma. Put

$$\mathcal{G} := \{R \mid R \text{ is a partial order on } S \text{ with } \leq \subseteq R\}$$

and order \mathcal{G} by inclusion. Let $\mathcal{C} \subseteq \mathcal{G}$ be a chain, then we claim that $R_0 := \bigcup \mathcal{C}$ is a partial order. It is obvious that R_0 is reflexive; if aR_0b and bR_0a , then there exists relations $R_1, R_2 \in \mathcal{C}$ with aR_1b and bR_2a . Since \mathcal{C} is a chain, we know that $R_1 \subseteq R_2$ or $R_2 \subseteq R_1$ holds. Assume that the former holds, then aR_2b follows, so that we may conclude $a = b$. Hence R_0 is antisymmetric. Transitivity is proved along the same lines, using that \mathcal{C} is a chain. By Zorn's Lemma, \mathcal{G} has a maximal element M ; since $M \in \mathcal{G}$, M is a partial order which contains the given partial order \leq .

We have to show that M is linear. Assume that it is not, so that there exists $a, b \in S$ such that both aMb and bMa are false. Put

$$M' := M \cup \{\langle x, y \rangle \mid xMa \text{ and } bMy\}.$$

Then M' contains M properly. If we can show that M' is a partial order, we have shown that M is not maximal, which is a contradiction. Let's see:

- M' is reflexive: Since $M \subseteq M'$ and M is reflexive, xMx holds for all $x \in S$.
- M' is transitive: Let $xM'y$ and $yM'z$, then these cases are possible
 1. xMy and yMz , hence xMz , thus $xM'z$.

2. xMy and yMa and bMz , thus xMa and bMz , so that $xM'z$.
3. xMa and bMy and yMz , hence $xM'z$.
4. xMa and bMy and yMa and bMz , but then bMa contrary to our assumption. Hence this case cannot occur.

Thus we may conclude that M' is transitive.

- M' is antisymmetric. Assume that $xM'y$ and $yM'x$, and look at the cases above with $z = x$. Case 2 would imply xMa and bMx , so is not possible, case 3 is excluded for the same reason, so only case 1 is left, which implies $x = y$.

Thus the assumption that there exists $a, b \in S$ such that both aMb and bMa are false leads to the conclusion that M is not maximal in \mathcal{G} , which is a contradiction.

Then $a <_s b$ iff $\langle a, b \rangle \in M$ defines the desired total order, and by construction it extends the given order.

Hence we have shown:

Proposition 1.50 *Each partial order on a set can be extended to a total order. \dashv*

1.5.3 Bases in Vector Spaces

Fix a vector space V over field K . A set $B \subseteq V$ is called *linear independent* iff $\sum_{b \in B_0} a_b \cdot b = 0$ implies $a_b = 0$ for all $b \in B_0$, whenever B_0 is a finite non-empty subset of B . Hence, e.g., a single vector v with $v \neq 0$ is linear independent.

Example 1.51 The reals \mathbb{R} form a vector space over the rationals \mathbb{Q} . Then $\sqrt{2}$ and $\sqrt{3}$ are independent. In fact, assume that $q_1\sqrt{2} + q_2\sqrt{3} = 0$ with rational numbers $q_1 = r_1/s_1$ and $q_2 = r_2/s_2$. Then we can find integers t_1, t_2 such that $t_1\sqrt{2} = t_2\sqrt{3}$ so that t_1 and t_2 have no common divisors. But $2t_1^2 = 3t_2^2$ implies that 2 and 3 are both common divisors to t_1 and to t_2 . \uparrow

The linear independent set B is called a *base* for V iff B is linear independent, and if each element $v \in V$ can be represented as

$$v = \sum_{i=1}^n a_i \cdot b_i$$

for some $a_1, \dots, a_n \in K$ and $b_1, \dots, b_n \in B$.

Proposition 1.52 *Each vector space V has a base.*

Proof 0. We first find a maximal independent set, and then we show that this set is a base.

1. Let

$$\mathcal{V} := \{B \subseteq V \mid B \text{ is linear independent}\}.$$

Then \mathcal{V} contains all singletons with non-null vectors, hence it is not empty. Order \mathcal{V} by inclusion, and let \mathcal{B} be a chain in \mathcal{V} . Then $B_0 := \bigcup \mathcal{B}$ is independent. In fact, if $\sum_{i=1}^n a_i \cdot b_i = 0$,

let $b_i \in B_i \in \mathcal{B}$ for $1 \leq i \leq n$. Since \mathcal{C} is linearly ordered, we find some k such that $b_i \in B_k$, since B_k is independent, we may conclude $b_1 = \dots = b_n = 0$. By Zorn's Lemma there exists a maximal independent set $B^* \in \mathcal{V}$.

2. If B^* is not a basis, then we find a vector x which cannot be represented as a finite linear combination of elements of B^* . Clearly $x \notin B^*$. But then $B^* \cup \{x\}$ is linear independent, for it could otherwise be represented by elements from B^* . This contradicts the maximality of B^* . \neg

One notes that part 1. of the proof could as well argue with the Maximality Principle, because a set is linear independent iff each finite subset is linear independent. Hence the set \mathcal{V} constructed in the proof is of finite character, hence contains by (MP) a maximal element. Then one argue exactly as in part 2. of the proof. This shows that (ZL) and (MP) are close relatives.

The proofs above not constructive, since they do not tell us how to construct a base for a given vector space, not even in the finite dimensional case.

1.5.4 Extending Linear Functionals

Sometimes one is given a linear map from a sub-vector space to the reals, and one wants to extend this map to a linear map on the whole vector space. Usually there is the constraint that both the given map and the extension should be dominated by a sub linear map.

Let V be a vector space over the reals. A map $f : V \rightarrow \mathbb{R}$ is said to be a *linear functional* (or a *linear map*) on V iff $f(\alpha \cdot x + \beta y) = \alpha \cdot f(x) + \beta \cdot f(y)$ holds for all $x, y \in V$ and $\alpha, \beta \in \mathbb{R}$. Thus a linear functional is compatible with the vector space structure of V . Call $p : V \rightarrow \mathbb{R}$ *sub linear* iff $p(x + y) \leq p(x) + p(y)$, and $p(\alpha \cdot x) = \alpha \cdot p(x)$ for all $x, y \in V$ and $\alpha \geq 0$.

We have a look at the situation in the finite dimensional case first.

Proposition 1.53 *Let V be a finite dimensional real vector space with a sub linear functional $p : V \rightarrow \mathbb{R}$. Given a subspace V_0 , and a linear map $f_0 : V_0 \rightarrow \mathbb{R}$ such that $f_0(x) \leq p(x)$ for all $x \in V_0$. Then there exists a linear functional $f : V \rightarrow \mathbb{R}$ which extends f_0 such that $f(x) \leq p(x)$ for all $x \in V$.*

Proof 1. It is enough to show that f_0 can be extended to a linear functional dominated by p to the vector space generated by $V_0 \cup \{z\}$ with $z \notin V_0$. In fact, we can then repeat this procedure a finite number of times, in each step adding a new basis vector not contained in the previous subspace. Since V is finite dimensional, this will eventually give us V as the domain for the linear functional.

2. Let $z \notin V_0$, then $\{v + \alpha \cdot z \mid v \in V_0, \alpha \in \mathbb{R}\}$ is the vector space generated by V_0 and z . This is clearly a vector space containing $V_0 \cup \{z\}$, and each vector space containing $V_0 \cup \{z\}$ must also contain linear combinations of the form $v + \alpha \cdot z$ with $v \in V_0$ and $\alpha \in \mathbb{R}$. Moreover, the representation of an element in this vector space is unique: assume $v + \alpha \cdot z = v' + \alpha' \cdot z$, then $v - v' = (\alpha - \alpha') \cdot z$, and because $z \notin V_0$, this implies $v - v' = 0$, hence also $\alpha = \alpha'$.

3. Now set

$$f(v + \alpha \cdot z) := f_0(v) + \alpha \cdot c$$

with a value c which will have to be determined. Consider $v, v' \in V_0$, then we have

$$f_0(v) - f_0(v') = f_0(v - v') \leq p(v - v') \leq p(v + z) + p(-z - v')$$

for an arbitrary $v_1 \in V$. Thus we obtain $-p(z - v') - f_0(v') \leq p(v + z) - f_0(v)$. Note that the left hand side of this inequality is independent of v , and that the right hand side is independent of v' , which means that we can find c with

- $c \leq p(v + z) - f_0(v)$ for all $v \in V_0$,
- $c \geq -p(-z - v') - f_0(v')$ for all $v \in V_0$.

Now let's see what happens. Fix α . If $\alpha = 0$, we have $f(v + 0 \cdot z) = f_0(v) \leq p(v + 0 \cdot z)$. If $\alpha > 0$, we have

$$f(v + \alpha \cdot z) = \alpha \cdot f(v/\alpha + z) = \alpha \cdot (f_0(v/\alpha) + c) \leq \alpha \cdot (f_0(v) + p(v/\alpha + z) - f_0(v/\alpha)) = p(v + \alpha \cdot z)$$

by (1.5.4) and sub linearity. If, however, $\alpha < 0$, we use the inequality (1.5.4) and sub linearity of p ; note that the coefficient $-z/\alpha$ of z is positive in this case.

Summarizing, we have $f(v + \alpha \cdot z) \leq p(v + \alpha \cdot z)$ for all $v \in V_0$ and $\alpha \in \mathbb{R}$. \dashv

When having a closer look at the proof, we see that the assumption on working in a finite dimensional vector space is only important for making sure that the extension process ends in a finite number of steps. The core of this proof, however, consists in the observation that we can extend a linear functional from a vector space V_0 to a vector space $\{v + \alpha \cdot z \mid v \in V_0, \alpha \in \mathbb{R}\}$ with $z \notin V_0$ without losing domination by the sub linear functional p . Let us record this important intermediate result.

Corollary 1.54 *Let V_0 be a vector space, $V_0 \subseteq V$, $p : V \rightarrow \mathbb{R}$ be a sub linear functional, and $z \notin V_0$. Then each linear functional $f : V_0 \rightarrow \mathbb{R}$ which is dominated by p can be extended to a linear functional f on the vector space generated by V_0 and z such that f is also dominated by p . \dashv*

Now we are in a position to formulate and prove the Hahn-Banach Theorem. We will use Zorn's Lemma for the proof by setting up a partial order such that each chain has an upper bound. We may conclude then that there exists a maximal element. By the "dimension free" version of the extension just stated we will then show that the assumption that we did not capture the whole vector space through our maximal element will yield a contradiction.

Theorem 1.55 *Let V be a real vector space with a sub linear functional $p : V \rightarrow \mathbb{R}$. Given a subspace V_0 , and a linear map $f_0 : V_0 \rightarrow \mathbb{R}$ such that $f_0(x) \leq p(x)$ for all $x \in V_0$. Then there exists a linear functional $f : V \rightarrow \mathbb{R}$ which extends f_0 such that $f(x) \leq p(x)$ for all $x \in V$.*

Proof 1. Define $\langle V', f' \rangle \in \mathcal{W}$ iff V' is a vector space with $V_0 \subseteq V' \subseteq V$, and $f' : V' \rightarrow \mathbb{R}$ extends f_0 and is dominated by p . Define $\langle V', f' \rangle \leq \langle V'', f'' \rangle$ iff V' is a subspace of V'' and f'' is an extension to f' for $\langle V', f' \rangle, \langle V'', f'' \rangle \in \mathcal{W}$. Then \leq is a partial order on \mathcal{W} . Let $(\langle V_i, f_i \rangle)_{i \in I}$ be a chain in \mathcal{W} , then $V' := \bigcup_{i \in I} V_i$ is a subspace of V . In fact, let $x, x' \in V'$, then $x \in V_i$ and $x' \in V_{i'}$. Then either $V_i \subseteq V_{i'}$ or $V_{i'} \subseteq V_i$. Assume the former, hence $x, x' \in V_{i'}$, thus $\alpha \cdot x + \beta \cdot x' \in V_{i'} \subseteq V'$ for all $\alpha, \beta \in \mathbb{R}$. Put $f'(x) := f_i(x)$, if $x \in V_i$ for some $i \in I$, then $f' : V' \rightarrow \mathbb{R}$ is well defined, linear and dominated by p , moreover, f' extends every f_i , hence, by transitivity, f_0 . This implies $\langle V', f' \rangle \in \mathcal{W}$, and this is obviously an upper bound for the chain.

2. Hence each chain has an upper bound in \mathcal{W} , so that Zorn's Lemma implies the existence of a maximal element $\langle V^+, f^+ \rangle \in \mathcal{W}$. Assume that $V^+ \neq V$, then there exists $z \in V$ with $z \notin V^+$. Then the vector space V^* generated by $V^+ \cup \{z\}$ contains V^+ properly, and f^+ has a linear extension f^* to V^* which is dominated by p by Corollary 1.54. But this means $\langle V^+, f^+ \rangle$ is strictly smaller than $\langle V^*, f^* \rangle \in \mathcal{W}$, a contradiction. Hence $V^+ = V$, and f^+ is the desired extension. \dashv

1.5.5 Maximal Filters

Fix a set S . The power set $\mathcal{P}(S)$ is ordered by inclusion, exhibiting some interesting properties.

Definition 1.56 A non-empty subset $\mathcal{F} \subseteq \mathcal{P}(S)$ is called a filter iff

1. $\emptyset \notin \mathcal{F}$,
2. if $F_1, F_2 \in \mathcal{F}$, then $F_1 \cap F_2 \in \mathcal{F}$,
3. if $F \in \mathcal{F}$ and $F \subseteq F'$, then $F' \in \mathcal{F}$.

Thus a filter is closed under finite intersections and closed with respect to super sets, and it must not contain the empty set.

Example 1.57 Given $s \in S$, the set $\mathcal{F}_s := \{A \subseteq S \mid s \in A\}$ is a filter. \mathbb{M}

Example 1.58 Let M be an infinite set. Then $\mathcal{F} := \{A \subseteq M \mid M \setminus A \text{ is finite}\}$ is a filter, the filter of cofinite sets. \mathbb{M}

The filter from Example 1.57 is special because it is maximal, we cannot find a filter \mathcal{G} which properly contains \mathcal{F}_s . Let's try: Take $G \in \mathcal{G}$ with $G \notin \mathcal{F}_s$, then $s \notin G$, hence $s \in S \setminus G$, so that both $G \in \mathcal{G}$ and $S \setminus G \in \mathcal{G}$, the latter one via \mathcal{F} . This implies $\emptyset \in \mathcal{G}$, since a filter is closed under finite intersections. We have arrived at a contradiction, giving rise to the definition of a maximal filter (Definition 1.62).

Before stating it, we will introduce filter bases. Sometimes we are not presented with a filter but rather with a family of sets which generates one.

Definition 1.59 A subset $\mathcal{B} \subseteq \mathcal{P}(S)$ is called a filter base iff no intersection of a finite collection of elements of \mathcal{B} is empty, thus iff $\emptyset \notin \{B_1 \cap \dots \cap B_n \mid B_1, \dots, B_n \in \mathcal{B}\}$.

Example 1.60 Fix $x \in \mathbb{R}$, then the set $\mathcal{B} := \{]a, b[\mid a < x < b\}$ of all open intervals containing x is a filter base. Let $(a_n)_{n \in \mathbb{N}}$ be a sequence in \mathbb{R} , then the set $\mathcal{E} := \{\{a_k \mid k \geq n\} \mid n \in \mathbb{N}\}$ of infinite tails of the sequence is a filter base as well. \mathbb{M}

Clearly, if \mathcal{B} is to be contained in a filter \mathcal{F} , then it must not have the empty sets among its finite intersections, because all these finite intersections are elements of \mathcal{F} . It is easy to characterize the filter generated by a base.

Lemma 1.61 Let \mathcal{B} be a filter base, then

$$\mathcal{F} := \{B \subseteq S \mid B \supseteq B_1 \cap \dots \cap B_n \text{ for some } B_1, \dots, B_n \in \mathcal{B}\}$$

is the smallest filter containing \mathcal{B} .

Proof It is clear that \mathcal{F} is a filter, because it cannot contain the empty set, it is closed under finite intersections, and it is closed under super sets. Let \mathcal{G} be a filter containing \mathcal{B} , and let $B \supseteq B_1 \cap \dots \cap B_n$ for some $B_1, \dots, B_n \in \mathcal{B} \subseteq \mathcal{G}$, hence $B \in \mathcal{G}$. Thus $\mathcal{F} \subseteq \mathcal{G}$, so that \mathcal{F} is in fact the smallest filter containing \mathcal{B} . \dashv

Let us return to the properties of the filter defined in Example 1.57.

Definition 1.62 A filter is called maximal iff it is not properly contained in another filter. Maximal filters are also called ultrafilters.

This is an easy characterization of maximal filters.

Lemma 1.63 These conditions are equivalent for a filter \mathcal{F}

1. \mathcal{F} is maximal.
2. For each subset $A \subseteq S$, either $A \in \mathcal{F}$ or $S \setminus A \in \mathcal{F}$.

Proof $1 \Rightarrow 2$: Assume there is a set $A \subseteq S$ such that both $A \notin \mathcal{F}$ and $S \setminus A \notin \mathcal{F}$ holds. Then

$$\mathcal{G}_0 := \{F \cap A \mid F \in \mathcal{F}\}$$

is a filter base, because $F \cap A = \emptyset$ for some $F \in \mathcal{F}$ would imply $F \subseteq S \setminus A$, thus $S \setminus A \in \mathcal{F}$. Because $F \cap A \notin \mathcal{F}$ for all $F \in \mathcal{F}$ we conclude that the filter \mathcal{G} generated by \mathcal{G}_0 contains \mathcal{F} properly. This \mathcal{F} is not maximal.

$2 \Rightarrow 1$: A filter \mathcal{G} which contains \mathcal{F} properly will contain a set $A \notin \mathcal{F}$. By assumption, $S \setminus A \in \mathcal{F} \subseteq \mathcal{G}$, so that $\emptyset \in \mathcal{G}$. \dashv

Example 1.64 The filter \mathcal{F} of cofinite sets from Example 1.58 for an infinite set M is not an ultrafilter. In fact, decompose $M = M_0 \cup M_1$ into disjoint sets M_0 and M_1 which are both infinite. Then neither M_0 nor its complement are contained in \mathcal{F} . \updownarrow

The existence of ultrafilters is trivial by Example 1.57, but we do not know whether each filter is actually contained in an ultrafilter. The answer is in the affirmative.

Theorem 1.65 Each filter can be extended to a maximal filter.

Proof Let \mathcal{F} be a filter on S , and define

$$\mathcal{V} := \{\mathcal{G} \mid \mathcal{G} \text{ is a filter with } \mathcal{F} \subseteq \mathcal{G}\}.$$

Order \mathcal{V} by inclusion. Then each chain \mathcal{C} in \mathcal{V} has an upper bound in \mathcal{V} . In fact, let $\mathcal{H} := \bigcup \mathcal{C}$. If $A \in \mathcal{H}$ and $A \subseteq B$, there exists a filter $\mathcal{G} \in \mathcal{C}$ with $A \in \mathcal{G}$, hence $B \in \mathcal{G}$, so that $B \in \mathcal{H}$. If $A, B \in \mathcal{H}$, we find $\mathcal{G}_A, \mathcal{G}_B \in \mathcal{H}$ with either $\mathcal{G}_A \subseteq \mathcal{G}_B$ or $\mathcal{G}_B \subseteq \mathcal{G}_A$, because \mathcal{C} is linearly ordered. Assume the former, hence $A, B \in \mathcal{G}_B$, hence $A \cap B \in \mathcal{G}_B \subseteq \mathcal{H}$. So \mathcal{H} is a filter in \mathcal{V} .

Thus there exists a maximal element \mathcal{F}^* which is a maximal filter (just repeat the argument in the proof of $2 \Rightarrow 1$ for Lemma 1.63). \mathcal{F}^* contains \mathcal{F} . \dashv

Corollary 1.66 Let $\emptyset \neq A \subseteq X$ be a non-empty subset of a set X . Then there exists an ultrafilter containing A .

Proof Using Theorem 1.65, extend the filter $\{B \subseteq X \mid A \subseteq B\}$ to an ultrafilter. \dashv

1.5.6 Ideals and Filters

Recall that a *lattice* (L, \leq) is an set L with an order relation \leq such that each non-empty finite subset has a lower bound and an upper bound. Put

$$\begin{aligned} a \wedge b &:= \inf\{a, b\}, \\ a \vee b &:= \sup\{a, b\}. \end{aligned}$$

We note these properties $(a, b \in L)$:

Idempotency $a \wedge a = a \vee a = a$.

Commutativity $a \wedge b = b \wedge a$ and $a \vee b = b \vee a$.

Absorption $a \wedge (a \vee b) = a$ and $a \vee (a \wedge b) = a$. In fact, $a \leq a \vee b$, thus $a = a \wedge a \leq a \wedge (a \vee b)$, on the other hand $a \wedge (a \vee b) \leq a$. The second equality is proved similarly.

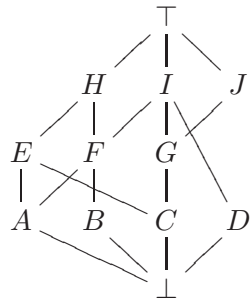
For simplicity we assume that the lattice is *bounded*, i.e., that it has a smallest element \perp and a largest element \top , so that we can put $\perp := \sup \emptyset$ and $\top := \inf \emptyset$, resp.

Example 1.67 The power set $\mathcal{P}(S)$ of a set S is a lattice, where $A \leq B$ iff $A \subseteq B$, so that

$$\begin{aligned} A \cap B &= \inf\{A, B\}, \\ A \cup B &= \sup\{A, B\}. \end{aligned}$$



Example 1.68 Look at this example




Then $\{B, C\}$ has these upper bounds: $\{\top, H, I\}$, thus has no smallest upper bound, so that — probably contrary to the first view — $B \vee C$ does not exist. trying to determine $A \vee B$, we see that the set of upper bounds to $\{A, B\}$ is just $\{\top, F, H, I\}$, hence $A \vee B = F$.



Example 1.69 Consider the set \mathcal{I} of all open intervals $]a, b[$ with $a, b \in \mathbb{R}$, and take the order inherited from $\mathcal{P}(\mathbb{R})$, then \mathcal{I} is closed under taking the infimum of two elements (since the intersection of two open intervals is again an open interval), but \mathcal{I} is not closed under taking the supremum of two elements in $\mathcal{P}(\mathbb{R})$, since the union of two open intervals is not necessarily an open interval. Nevertheless, \mathcal{I} is a lattice in its own right, because we have

$$]a_1, b_1[\vee]a_2, b_2[=]\min\{a_1, a_2\}, \max\{b_1, b_2\}[$$

in \mathcal{I} . Hence we have to be careful where to look for the supremum. 

Example 1.70 Similarly, consider the set \mathcal{R} of all closed rectangles in the plane $\mathbb{R} \times \mathbb{R}$, again with the order inherited from $\mathcal{P}(\mathbb{R} \times \mathbb{R})$. The intersection $R_1 \cap R_2$ of two closed rectangles $R_1, R_2 \in \mathcal{R}$ is an element of \mathcal{R} and is indeed the infimum of R_1 and R_2 . But what do we take as the supremum in \mathcal{R} , if it exists at all? From the definition of the supremum we have

$$R_1 \vee R_2 = \bigcap \{R \in \mathcal{R} \mid R_1 \subseteq R \text{ and } R_2 \subseteq R\},$$

in plain words, the smallest closed rectangle which encloses both R_1 and R_2 . Hence, e.g.,

$$[0, 1] \times [0, 1] \vee [5, 6] \times [8, 9] = [0, 6] \times [0, 9].$$

This renders \mathcal{R} a lattice indeed. \mathfrak{M}

A lattice is called *distributive* iff

$$\begin{aligned} a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c) \\ a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c) \end{aligned}$$

holds (both equations are actually equivalent, see Exercise 23).

Example 1.71 The powerset lattice $\mathcal{P}(S)$ is a distributive lattice, because unions and intersections are distributive.

But BEWARE! Distributivity is not necessarily inherited. Consider the lattice \mathcal{J} of closed intervals of the real line, as in Example 1.69, then

$$\begin{aligned} I_1 \wedge I_2 &= I_1 \cap I_2, \\ I_1 \vee I_2 &= [\min I_1 \cup I_2, \max I_1 \cup I_2], \end{aligned}$$

as above. Put $A := [-3, -2], B := [-1, 1], C := [2, 3]$, then

$$\begin{aligned} (A \wedge B) \vee (B \wedge C) &= \emptyset, \\ B \wedge (A \vee C) &= [-1, 1]. \end{aligned}$$

Thus \mathcal{J} is not distributive, although the order has been inherited from the powerset. \mathfrak{M}

Example 1.72 Let P be a set with a partial order \leq . A set $D \subseteq P$ is called a *down set* iff $t \in D$ and $s \leq t$ imply $s \in D$. Hence a down set is downward closed in the sense that all elements below an element of the set belong to the set as well. A generic example for a down set is $\{s \in P \mid s \leq t\}$ with $t \in P$. Down sets of this shape are called *principal down sets*. The intersection and the union of two down sets are down sets again. For example, let D_1 and D_2 be down sets, let $t \in D_1 \cup D_2$, and assume $s \leq t$. Because $t \in D_1$ or $t \in D_2$ we may conclude that $s \in D_1$ or $s \in D_2$, hence $s \in D_1 \cup D_2$. Let $\mathcal{D}(P)$ be the set of all down sets of P , then $\mathcal{D}(P)$ is a distributive lattice; this is so because the infimum and the supremum of two elements in $\mathcal{D}(P)$ are the same as in $\mathcal{P}(P)$.

Define

$$\Psi : \begin{cases} P & \rightarrow \mathcal{D}(P) \\ t & \mapsto \{s \in P \mid s \leq t\} \end{cases}$$

Then $t_1 \leq t_2$ implies $\Psi(t_1) \subseteq \Psi(t_2)$, hence the order structure carries over from P to $\mathcal{D}(P)$. Moreover $\Psi(t_1) = \Psi(t_2)$ implies $t_1 = t_2$, so that Ψ is injective. Hence we have embedded the partially ordered set P into a distributive lattice. \mathfrak{M}

A *Boolean algebra* B is a distributive lattice such that there exists a unary operation $- : B \rightarrow B$ such that

$$a \vee -a = \top$$

$$a \wedge -a = \perp$$

$-a$ is called the complement of a . We assume that \wedge binds stronger than \vee , and that complementation binds stronger than the binary operations.

Filters and ideals are important structures in a lattice.

Definition 1.73 Let L be a lattice.

$J \subseteq L$ is called an *ideal* iff

- $\emptyset \neq J \neq L$.
- If $a, b \in J$, then $a \vee b \in J$.
- If $a \in J$ and $b \in L$ with $b \leq a$, then $b \in J$.

$F \subseteq L$ is called a *filter* iff

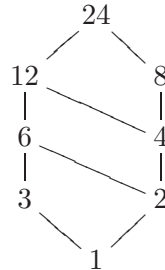
- $\emptyset \neq F \neq L$.
- If $a, b \in F$, then $a \wedge b \in F$.
- If $a \in F$ and $b \in L$ with $b \geq a$, then $b \in F$.

The ideal J is called *prime* iff $a \wedge b \in J$ implies $a \in J$ or $b \in J$, it is called *maximal* iff it is not properly contained in another ideal. The filter F is called *prime* iff $a \vee b \in F$ implies $a \in F$ or $b \in F$, it is called *maximal* iff it is not properly contained in another filter.

Maximal filters are also called *ultrafilters*. Recall the definition of an ultrafilter in Definition 1.62; we have defined already ultrafilters for the special case that the underlying Boolean algebra is the power set of a given set. The notion of a filter base fortunately carries over directly from Definition 1.59, so that we may use Lemma 1.61 in the present context as well. We will be in this section a bit more general, but first some simple examples.

Example 1.74 $I := \{F \subseteq \mathbb{N} \mid F \text{ is finite}\}$ is an ideal in $\mathcal{P}(\mathbb{N})$ with set inclusion as the partial order. This is so since the intersection of two finite sets is finite again, and because subsets of finite sets are finite again. Also $\emptyset \neq I \neq \mathcal{P}(\mathbb{N})$. This ideal is not prime. \mathfrak{M}

Example 1.75 Consider all divisors of 24.



$\{1, 2, 3, 6\}$ is an ideal, $\{1, 2, 3, 4, 6\}$ is not. \mathfrak{M}

Example 1.76 Let $S \neq \emptyset$ be a set, $a \in S$. Then $\mathcal{P}(S \setminus \{a\})$ is a prime ideal in $\mathcal{P}(S)$ (with set inclusion as the partial order). In fact, $\emptyset \neq \mathcal{P}(S \setminus \{a\}) \neq \mathcal{P}(S)$, and if $a \notin A$ and $a \notin B$, then $a \notin A \cup B$. On the other hand, if $a \notin A \cap B$, then $a \notin A$ or $a \notin B$. \mathfrak{M}

Lemma 1.77 Let L be a lattice, $\emptyset \neq F \neq L$ be a proper non-empty subset of L .

- These conditions are equivalent

1. F is a filter.

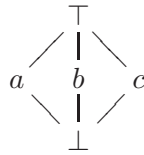
2. $\top \in F$ and $(a \wedge b \in F \Leftrightarrow a \in F \text{ and } b \in F)$.

- If filter F is maximal and L is distributive, then F is a prime filter

Proof 1. The implication $1 \Rightarrow 2$ in the first part is trivial, for $2 \Rightarrow 1$ one notes that $a \leq b$ is equivalent to $a \wedge b = a$.

2. In order to show that the maximal filter F is prime, we show that $a \vee b \in F$ implies $a \in F$ or $b \in F$. Assume that $a \vee b \in F$ with $a \notin F$. Consider $B := \{f \wedge b \mid f \in F\}$, then $\perp \notin B$. In fact, assume that $f \vee b = \perp$ for some $f \in F$, then we could write $a = (f \wedge b) \vee a = (f \vee a) \wedge (b \vee a)$ by distributivity. Since $f \in F$ and F is a filter, $f \vee a \in F$ follows, and since $b \vee a \in F$, we obtain $a \in F$, contradicting the assumption. Thus B is a filter base, and because F is maximal we may conclude that $B \subseteq F$, which in turn implies $b \in F$. \dashv

Hence maximal filters are prime in a distributive lattice. If the lattice is not distributive, this may not be true. Look at this example



The lattice is not distributive, because $(a \wedge b) \vee c = c \neq \top = (a \vee c) \wedge (b \vee c)$. Then $\{\top\}$, $\{\top, a\}$, $\{\top, b\}$, $\{\top, c\}$ and $\{\top, d\}$ are filters, $\{\top, a\}$, $\{\top, b\}$, $\{\top, c\}$ are maximal, but none of them is prime.

Prime ideals and prime filters are not only dual notions, they are also complementary concepts.

Lemma 1.78 In a lattice L a subset F is a prime filter iff its complement $L \setminus F$ is a prime ideal.

Proof Exercise 15. \dashv

We can say more in a Boolean algebra:

Lemma 1.79 Let B be a Boolean algebra. Then an ideal is maximal iff it is prime, and a filter is maximal iff it is prime.

Proof Note that a Boolean algebra is a distributive lattice with more than one element (viz., \perp and \top). We prove the assertion only for filters. That a maximal filter is prime has been shown in Lemma 1.77. If \mathcal{F} is not maximal, there exists a with $a \notin \mathcal{F}$ and $-a \notin \mathcal{F}$ by Lemma 1.63. But $\top = a \vee -a \in \mathcal{F}$, hence \mathcal{F} is not prime. \dashv

This is another and probably surprising equivalent to (AC).

(MII) Each lattice with more than one element contains a maximal ideal.

Theorem 1.80 (MII) is equivalent to (AC).

Proof 1. (MII) \Rightarrow (AC): We show actually that (MII) implies (MP), an application of Theorem 1.45 will then establish the claim. Let $\mathcal{F} \subseteq \mathcal{P}(S)$ be a family of finite character. In

order to apply (MII), we need a lattice L , which we will define now. Define $\mathcal{L} := \mathcal{F} \cup \{S\}$, and put for $X, Y \in \mathcal{F}$

$$X \wedge Y := X \cap Y,$$

$$X \vee Y := \begin{cases} X \cup Y, & \text{if } X \cup Y \in \mathcal{F}, \\ S, & \text{otherwise} \end{cases}$$

Then \mathcal{L} is a lattice with top element S and bottom element \emptyset . Let \mathcal{M} be a maximal ideal in \mathcal{L} , then we assert that $M^* := \bigcup \mathcal{M}$ is a maximal element of \mathcal{F} . Then $M^* \neq S$.

First we show that $M^* \in \mathcal{F}$. If $\{a_1, \dots, a_k\} \in M^*$, then we can find $M_i \in \mathcal{M}$ such that $m_i \in M_i$ for $1 \leq i \leq k$. Since \mathcal{M} is an ideal in \mathcal{L} , we know that $M_1 \vee \dots \vee M_k \in \mathcal{M}$, so that $\{a_1, \dots, a_k\} \in \mathcal{F}$, hence $M^* \in \mathcal{F}$.

Now assume that M^* is not maximal, then we can find $N \in \mathcal{F}$ such that M^* is a proper subset of N , hence there exists $t \in N$ such that $t \notin M^*$. Because $N \in \mathcal{F}$ and \mathcal{F} is of finite character, $\{t\} \in \mathcal{F}$. Now put $\mathcal{M}' := \mathcal{M} \cup \{M \vee \{t\} \mid M \in \mathcal{M}\} = \mathcal{M} \cup \{M \cup \{t\} \mid M \in \mathcal{M}\}$, then \mathcal{M}' is an ideal in \mathcal{L} which properly contains \mathcal{M} . This is a contradiction, hence we have found a maximal element of \mathcal{F} .

2. (AC) \Rightarrow (MII): Again, we use the equivalences in Theorem 1.45, because we actually show (ZL) \Rightarrow (MII). Let L be a lattice with at least two elements, and order

$$\mathcal{I} := \{I \subseteq L \mid I \text{ is an ideal in } L\}$$

by inclusion. Because $\{b \in L \mid b \leq a\} \in \mathcal{I}$ for $a \in L, a \neq \top$ (by assumption, such an element exists), we know that $\mathcal{I} \neq \emptyset$. If $\mathcal{C} \subseteq \mathcal{I}$ is a chain, then $I := \bigcup \mathcal{C} \in \mathcal{I}$. In fact, $\emptyset \neq I \neq L$, because $\top \notin I$, and if $a, b \in I$, we find I_1, I_2 with $a \in I_1, b \in I_2$, because \mathcal{C} is a chain, we may assume that $I_1 \subseteq I_2$, hence $a, b \in I_2$, so that $a \vee b \in I_2 \subseteq I$. If $a \leq b$ and $b \in I$ then $a \in I$, because $b \in I_1$ for some $I_1 \in \mathcal{I}$. Hence each chain has an upper bound in \mathcal{I} . (ZL) implies the existence of a maximal element $M \in \mathcal{I}$. \dashv

Since each Boolean algebra is a lattice with more than the top element, the following corollary is a consequence of Theorem 1.80. It is known under the name *Prime Ideal Theorem*. We know from Lemma 1.79 that prime ideals and maximal ideals are really the same.

Corollary 1.81 (AC) *implies the existence of a prime ideal in a Boolean algebra.* \dashv

1.5.7 The Stone Representation Theorem

Let us stick for a moment to Boolean algebras and discuss the famous Stone Representation Theorem, which requires the Prime Ideal Theorem at a crucial point.

Fix a Boolean algebra B and define for two elements $a, b \in B$ their *symmetric difference* $a \oplus b$ through

$$a \oplus b := (a \wedge -b) \vee (-a \wedge b)$$

If $B = \mathcal{P}(S)$ for some set S , and if $\wedge, \vee, -$ are the respective set operations $\cap, \cup, S \setminus \cdot$, then $A \oplus B$ is in fact equal to the symmetric difference $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (B \cap A)$.

Fix an ideal I of B , and define

$$a \sim_I b \Leftrightarrow a \ominus b \in I$$

Then \sim_I is a congruence, i.e., an equivalence relation which is compatible with the operations on the Boolean algebra. This will be shown now through a sequence of statements.

We state some helpful properties.

Lemma 1.82 *Let B be a Boolean algebra, then*

1. $a \ominus a = \perp$, $a \ominus b = b \ominus a$ and $a \ominus b = (-a) \ominus (-b)$.
2. $a \ominus b = (a \vee b) \wedge -(a \wedge b)$.
3. $(a \ominus b) \wedge c = (a \wedge c) \ominus (b \wedge c)$ and $c \wedge (a \ominus b) = (c \wedge a) \ominus (c \wedge b)$.

Proof The properties under 1. are fairly obvious, 2. is calculated directly using distributivity, finally the first part of 3. follows thus

$$\begin{aligned} (a \wedge c) \ominus (b \wedge c) &= (a \wedge c \wedge -(b \wedge c)) \vee (b \wedge c \wedge -(a \wedge c)) \\ &= (a \wedge c \wedge (-b \vee -c)) \vee (b \wedge c \wedge (-a \vee -c)) \\ &= (a \wedge -b \wedge c) \vee (b \wedge -a \wedge c) \\ &= (a \ominus b) \wedge c, \end{aligned}$$

because $a \wedge c \wedge -c = \perp = b \wedge c \wedge -c$. \dashv

Lemma 1.83 \sim_I is an equivalence relation on B with these properties

1. $a \sim_I a'$ and $b \sim_I b'$ imply $a \wedge b \sim_I a' \wedge b'$ and $a \vee b \sim_I a' \vee b'$.
2. $a \sim_I a'$ implies $-a \sim_I -a'$.

Proof Because $a \ominus a' \in I$ and $b \ominus b' \in I$ we conclude that $(a \ominus a') \vee (b \ominus b') \in I$, thus

$$\begin{aligned} (a \vee a') \ominus (b \vee b') &\leq ((a \vee b) \wedge -(a \wedge b)) \vee ((a' \vee b') \wedge -(a' \wedge b')) \\ &= (a \ominus a') \vee (b \ominus b') \in I. \end{aligned}$$

Since I is an ideal, we conclude $(a \vee a') \ominus (b \vee b') \in I$.

From Lemma 1.82 we conclude that $a \wedge b \sim_I a' \wedge b \sim_I a' \wedge b'$. The assertion about complementation follows from Lemma 1.82 as well. \dashv

Denote by $[x]_{\sim_I}$ the equivalence class of $x \in B$, and let $\eta_{\sim_I} : x \mapsto [x]_{\sim_I}$ be the associated factor map. Define on the factor space $B/I := \{[x]_{\sim_I} \mid x \in B\}$ the operations

$$\begin{aligned} [a]_{\sim_I} \wedge [b]_{\sim_I} &:= [a \wedge b]_{\sim_I}, \\ [a]_{\sim_I} \vee [b]_{\sim_I} &:= [a \vee b]_{\sim_I}, \\ -[a]_{\sim_I} &:= [-a]_{\sim_I}. \end{aligned}$$

We have also

$$\begin{aligned} [a]_{\sim_I} \leq [b]_{\sim_I} &\Leftrightarrow a \ominus (a \wedge b) \in I \Leftrightarrow b \ominus (a \vee b) \in I, \\ a \in I &\Leftrightarrow a \sim_I \perp. \end{aligned}$$

The following statement is now fairly easy to prove. Recall that a homomorphism $f : (B, \wedge, \vee, -) \rightarrow (B', \wedge', \vee', -')$ is a map $f : B \rightarrow B'$ such that $f(a \wedge b) = f(a) \wedge' f(b)$, $f(a \vee b) = f(a) \vee' f(b)$ and $f(-a) = -'f(a)$ for all $a, b \in B$ are valid.

Proposition 1.84 *The factor space B/I is a Boolean algebra, and η_{\sim_I} is a homomorphism of Boolean algebras.*

Proof The operations on B/I are well defined by Lemma 1.83 and yield a lattice with $[\top]_{\sim_I}$ as the largest and $[\perp]_{\sim_I}$ as the smallest element, resp. Hence $-$ is a complementation operator on B/I because

$$\begin{aligned} [a]_{\sim_I} \wedge [-a]_{\sim_I} &= [\perp]_{\sim_I}, \\ [a]_{\sim_I} \vee [-a]_{\sim_I} &= [\top]_{\sim_I}. \end{aligned}$$

It is evident from the construction that η_{\sim_I} is a homomorphism. \dashv

The Prime Ideal Theorem implies that the Boolean algebra B/I has a prime ideal J by Corollary 1.81. This observation leads to a stronger version of this theorem for the given Boolean algebra.

Theorem 1.85 *Let I be an ideal in a Boolean algebra. Then $(\mathbb{A}\mathbb{C})$ implies that there exists a prime ideal K which contains I .*

Proof 1. Construct the factor algebra B/I , then $(\mathbb{A}\mathbb{C})$ implies that this Boolean algebra has a prime ideal J . We claim that

$$K := \{x \in B \mid [x]_{\sim_I} \in J\}$$

is the desired prime ideal. Since $I = [\perp]_{\sim_I} \in J$, we see that $I \subseteq K$ holds, thus $K \neq \emptyset$.

2. K is an ideal. If $K = B$, then $\top \in K$ which would mean $[\top]_{\sim_I} \in J$, but this is impossible. Let $a \leq b$ with $b \in K$, hence $a = a \wedge b$, so that $[a]_{\sim_I} = [a \wedge b]_{\sim_I}$. Because $b \in K$, we infer $[a \wedge b]_{\sim_I} \in J$, hence $[a]_{\sim_I} \in J$, so that $a \in K$. If $a, b \in K$, then $a \vee b \in K$, because J is an ideal.

3. K is prime. In fact, we have

$$\begin{aligned} a \wedge b \in K &\Leftrightarrow [a \wedge b]_{\sim_I} \in J \Leftrightarrow [a]_{\sim_I} \wedge [b]_{\sim_I} \in J \\ &\Rightarrow [a]_{\sim_I} \in J \text{ or } [b]_{\sim_I} \in J \Leftrightarrow a \in K \text{ or } b \in K \end{aligned}$$

\dashv

As a consequence, we can find in a Boolean algebra for any given element $a \neq \top$ a prime ideal which does contain it.

Corollary 1.86 *Let B be a Boolean algebra and assume that $(\mathbb{A}\mathbb{C})$ holds.*

1. *Given $a \neq \top$, there exists a prime ideal which contains a .*
2. *Given $a, b \in B$ with $a \neq b$, there exists a prime ideal which contains a but not b .*

3. Given $a, b \in B$ with $a \neq b$, there exists an ultrafilter which contains a but not b .

Proof We find a prime ideal K which extends the ideal $\{x \in B \mid x \leq a\}$. This establishes the first part.

If $a \neq b$, we have $a \ominus b \neq \perp$, so $a \wedge -b \neq \perp$ or $-a \wedge b \neq \perp$. Assume the former, then there exists a prime ideal K with $-(a \wedge -b) \in K$, so that both $b \in K$ and $-a \in K$ holds. Since $-a \in K$ implies $a \notin K$, we are done with the second part. The third part follows through Lemma 1.78. \dashv

This yields one of the true classics, the Stone Representation Theorem. It states that each Boolean algebra is essentially a set algebra, i.e., a Boolean algebra comprised of sets.

Theorem 1.87 *Let B be a Boolean algebra, and assume that $(\mathbb{A}\mathbb{C})$ holds. Then there exists a Boolean set algebra S such that B is isomorphic to S .*

Proof Define

$$\begin{aligned}\mathcal{S}_0 &:= \{U \mid U \text{ is an ultrafilter on } B\}, \\ \psi(b) &:= \{U \in \mathcal{S}_0 \mid b \in U\}.\end{aligned}$$

Then

$$\begin{aligned}\psi(b_1 \wedge b_2) &= \psi(b_1) \cap \psi(b_2), \\ \psi(b_1 \vee b_2) &= \psi(b_1) \cup \psi(b_2), \\ \psi(-b) &= \mathcal{S}_0 \setminus \psi(b).\end{aligned}$$

For example, we obtain from Lemma 1.77 that

$$\begin{aligned}U \in \psi(b_1 \wedge b_2) &\Leftrightarrow b_1 \wedge b_2 \in U \\ &\Leftrightarrow b_1 \in U \text{ and } b_2 \in U \\ &\Leftrightarrow U \in \psi(b_1) \text{ and } U \in \psi(b_2) \\ &\Leftrightarrow U \in \psi(b_1) \cap \psi(b_2).\end{aligned}$$

Similarly, $U \in \psi(-b) \Leftrightarrow -b \in U \Leftrightarrow b \notin U \Leftrightarrow U \notin \psi(b)$ by Lemma 1.63, because U is an ultrafilter.

Because we can find for $b_1 \neq b_2$ an ultrafilter which contains b_1 but not b_2 by Corollary 1.86, we conclude that ψ is injective (this is actually the place where $(\mathbb{A}\mathbb{C})$ is used). Thus the Boolean algebras B and $\psi[B]$ are isomorphic, and the latter one is comprised of sets. \dashv

1.5.8 Compactness and Alexander's Subbase Theorem

The closed interval $[u, v]$ with $-\infty < u < v < +\infty$ is an important example of a compact space. It has the following property: each cover through a countable number of open intervals contains a finite subcover which already cover the interval. This is what the famous Heine-Borel Theorem states. We give below Borel's proof [Fic64, vol. I, p. 163].

This section assumes that $(\mathbb{A}\mathbb{C})$ holds.

We will prove in this section Alexander's Subbase Theorem as an application for Zorn's Lemma. The Theorem states that when proving a space compact one may restrict one's attention to a particular subclass of open sets, a class which is usually easier to handle than the full family of open sets. This application of Zorn's Lemma is interesting because it shows in which way a maximality argument can be used for establishing a property through a subclass (rather than extending a property until maximality puts a stop to it, as we did in showing that each vector space has a basis). Alexander's Theorem is also a very practical tool, as we will see later.

This is the Heine-Borel Theorem.

Theorem 1.88 *Let an interval $[u, v]$ with $-\infty < u < v < +\infty$ be given. Then each cover $\{]x_n, y_n[\mid n \in \mathbb{N}\}$ of $[u, v]$ through a countable number of open intervals contains a finite cover $]x_{n_1}, y_{n_1}[, \dots,]x_{n_k}, y_{n_k}[$.*

Proof Suppose the assertion is false, then either $[u, 1/2(u+v)]$ or $[1/2(u+v), v]$ is not covered by finitely many of those intervals; select the corresponding one, call it $[a_1, b_1]$. This interval can be halved, let $[a_2, b_2]$ be the half which cannot be covered by finitely many intervals. Repeating this process, one obtains a sequence $\{[a_n, b_n] \mid n \in \mathbb{N}\}$ of intervals, each having half of the length of its predecessor, and each one not being covered by a finite number of intervals from $\{]x_n, y_n[\mid n \in \mathbb{N}\}$. Because the lengths of the intervals shrink to zero, there exists $c \in [u, v]$ with $\lim_{n \rightarrow \infty} a_n = c = \lim_{n \rightarrow \infty} b_n$, hence $c \in]x_m, y_m[$ for some m . But there is some $n_0 \in \mathbb{N}$ with $[a_n, b_n] \subseteq]x_m, y_m[$ for $n \geq n_0$, contradicting the assumption that $[a_n, b_n]$ cannot be covered by a finite number of those intervals. \dashv

Although the proof is given for a countable cover, its analysis shows that it goes through for an arbitrary cover of open intervals (this is so because each cover induces a partition of the interval considered into two parts, so a sequence of intervals will result in any case). This section will discuss compact spaces which have the property that an arbitrary cover contains a finite one. To be on firm ground, we first introduce topological spaces as the kind of objects to be discussed here.

Definition 1.89 *Given a set X , a subset $\tau \subseteq \mathcal{P}(X)$ is called a topology iff these conditions are satisfied:*

- $\emptyset, X \in \tau$.
- If $G_1, \dots, G_k \in \tau$, then $G_1 \cap \dots \cap G_k \in \tau$, thus τ is closed under finite intersections.
- If $\tau_0 \subseteq \tau$, then $\bigcup \tau_0 \in \tau$, thus τ is closed under arbitrary unions.

The pair (X, τ) is then called a topological space, the elements of τ are called open sets. An open neighborhood U of an element $x \in X$ is an open set U with $x \in U$.

These are the topologies one can always find on a set X .

Example 1.90 $\mathcal{P}(X)$ and $\{\emptyset, X\}$ are always topologies; the former one is called the *discrete topology*, the latter one is called *indiscrete*. \mathbb{N}

The topology one deals with usually on the reals is given by intervals, and the plane is topologically described by open balls (well, they really are circles, but they are given through measuring a distance, and in this case the name "ball" sticks).

Example 1.91 Call a set $G \subseteq \mathbb{R}$ open iff for each $x \in G$ there exists $a, b \in \mathbb{R}$ with $a < b$ such that $x \in]a, b[\subseteq G$; note that \emptyset is open. Then the open sets form a topology on the reals, which is also called the *interval topology*. Clearly, G is open iff, given $x \in G$, there exists $\epsilon > 0$ with $]x - \epsilon, x + \epsilon[\subseteq G$. Call a subset $G \subseteq \mathbb{R}^2$ of the Euclidean plane open iff, given $x \in G$, there exists $\epsilon > 0$ such that $B_\epsilon(x) \subseteq G$, where $B_r(x_1, x_2) := \{ \langle y_1, y_2 \rangle \mid \sqrt{(y_1 - x_1)^2 + (y_2 - x_2)^2} < r \}$ is the open ball centered at $\langle x_1, x_2 \rangle$ with radius r . \upharpoonright

Let (X, τ) be a topological space. If $Y \subseteq X$, then the trace of τ on Y gives a topology τ_Y on Y , formally, $\tau_Y := \{G \cap Y \mid G \in \tau\}$, the *subspace topology*. This permits sometimes to transfer a property from the space to its subsets.

A set $F \subseteq X$ is called *closed* iff its complement $X \setminus F$ is open. Then both \emptyset and X are closed, and the closed sets are closed (no pun intended) under arbitrary intersections and finite unions. We associate with each set an open set and a closed set:

Definition 1.92 Let $M \subseteq X$, then

- $M^\circ := \bigcup \{G \in \tau \mid G \subseteq M\}$ is called the interior of M .
- $M^a := \bigcap \{F \subseteq X \mid M \subseteq F \text{ and } F \text{ is closed}\}$ is called the closure of M .
- $\partial M := M^a \setminus M^\circ$ is called the boundary of M .

We have always $M^\circ \subseteq M \subseteq M^a$; this is apparent from the definition. Clearly, M° is an open set, and it is the largest open set which is contained in M , so that M is open iff $M = M^\circ$. Similarly, M^a is a closed set, and it is the smallest closed set which contains M . We also have M is closed iff $M = M^a$. The boundary ∂M is also a closed set, because it is the intersection of two closed sets, and we have $\partial M = \partial X \setminus M$. M is closed iff $\partial M \subseteq M$. All this is easily established through the definitions.

Look at the indiscrete topology: Here we have $\{x\}^\circ = \emptyset$ and $\{x\}^a = X$ for each $x \in X$. For the discrete topology one sees $A^\circ = A^a = A$ for each $A \subseteq X$.

Example 1.93 In the Euclidean topology on \mathbb{R}^2 of Example 1.91, we have

$$\begin{aligned} B_r(x_1, x_2)^a &= \{ \langle y_1, y_2 \rangle \mid \sqrt{(y_1 - x_1)^2 + (y_2 - x_2)^2} \leq r \}, \\ \partial B_r(x_1, x_2) &= \{ \langle y_1, y_2 \rangle \mid \sqrt{(y_1 - x_1)^2 + (y_2 - x_2)^2} = r \}. \end{aligned}$$

\upharpoonright

Just to get familiar with boundaries:

Lemma 1.94 Let (X, τ) be a topological space, $A \subseteq X$. Then $x \in \partial A$ iff each neighborhood of x has a non-empty intersection with A and with $X \setminus A$. In particular $\partial A = \partial(X \setminus A)$ and $\partial(A \cup B) \subseteq (\partial A) \cup (\partial B)$.

Proof Let $x \in \partial A$, and U an open neighborhood of x . If $A \cap U = \emptyset$, then $A \subseteq X \setminus U$, so $x \notin A^a$, if $U \cap X \setminus A = \emptyset$, it follows $x \in A^\circ$. So we arrive at a contradiction. Assume that $x \in \bigcap \{U \mid x \in U, U \cap A \neq \emptyset, U \cap X \setminus A \neq \emptyset\}$, then $x \notin A^\circ$, similarly, $x \notin X \setminus A^\circ = X \setminus (A^a)$. \dashv

A set without a boundary is both closed and open, so it is called *clopen*. The clopen sets of a topological space form a Boolean algebra.

Sometimes it is sufficient to describe the topology in terms of some special sets, like the open balls for the Euclidean topology.

Definition 1.95 A subset $\mathcal{B} \subseteq \tau$ of the open sets is called a *base* for the topology iff for each open set $G \in \tau$ and for each $x \in G$ there exists $B \in \mathcal{B}$ such that $x \in B \subseteq G$, thus each open set is the union of all base elements contained in it. $\mathcal{S} \subseteq \tau$ is called a *subbase* for τ iff the set of finite intersections of elements of \mathcal{S} forms a base for τ .

Then the open intervals are a base for the interval topology, and the open balls are a base for the Euclidean topology (actually, we did introduce the respective topologies through their bases). A subbase for the interval topology is given by the sets $\{] - \infty, a[\mid a \in \mathbb{R} \}$, because the set of finite intersections includes all open intervals, which in turn form a base. Bases and subbases are not uniquely determined, for example $\{]r, s[\mid r < s, r, s \in \mathbb{Q} \}$ is a base for the interval topology.

Let us return to the problem discussed in the opening of this section. We have seen that finite open intervals have the remarkable property that, whenever we cover them by an arbitrary number of open intervals, we can find a finite collection among these intervals which already cover the interval. This property can be generalized to arbitrary topological spaces; subsets with this properties are called *compact*, formally:

Definition 1.96 The topological space (X, τ) is called *compact* iff each cover of X by open sets contains a finite subcover.

Thus X is compact iff, whenever $(G_i)_{i \in I}$ is a collection of open sets with $X = \bigcup_{i \in I} G_i$, there exists $I_0 \subseteq I$ finite such that $X \subseteq \bigcup_{i \in I_0} G_i$. It is apparent that compactness is a generalization of finiteness, so that compact sets are somewhat small, measured in terms of open sets. Consider as a trivial example the discrete topology. Then X is compact precisely when X is finite.

This is an easy consequence of the definition.

Lemma 1.97 Let (X, τ) be a compact topological space, and $F \subseteq X$. Then F is compact (thus (F, τ_F) is a compact topological space). \dashv

The following example shows a close connection of Boolean algebras to compact topological spaces; this is the famous *Stone Duality Theorem*.

Example 1.98 Let B be a Boolean algebra with \wp_B as the set of all prime ideals of B . Define

$$X_a := \{ I \in \wp_B \mid a \notin I \}.$$

Then we have these properties

- $X_{\top} = \wp_B$, since an ideal does not contain \top .
- $X_{-a} = \wp_B \setminus X_a$. To see this, let I be a prime filter, then $I \in X_{-a}$ iff $-a \notin I$, this is the case iff $-a \in B \setminus I$, hence iff $a \notin B \setminus I$, since $B \setminus I$ is a maximal filter by Lemma 1.78 and Lemma 1.79; the latter condition is equivalent to $a \in I$, hence to $I \notin X_a$.
- $X_{a \wedge b} = X_a \cap X_b$ and $X_{a \vee b} = X_a \cup X_b$. This follows similarly from Lemma 1.77.

Define a topology τ on \wp_B by taking the sets X_a as a base, formally

$$\mathcal{B} := \{X_a \mid a \in B\}.$$

We claim that (\wp_B, τ) is compact. In fact, let \mathcal{U} be a cover of \wp_B with open sets. Because each $U \in \mathcal{U}$ can be written as a union of elements of \mathcal{B} , we may and do assume that $\mathcal{U} \subseteq \mathcal{B}$, so that $\mathcal{U} = \{X_a \mid a \in A\}$ for some $A \subseteq B$. Now let J be the ideal generated by A , so that J can be written as

$$J := \{b \in B \mid b \leq a_1 \vee \dots \vee a_k \text{ for some } a_1, \dots, a_k \in A\}.$$

We distinguish these cases:


$\top \in J$: In this case we have $\top = a_1 \vee \dots \vee a_k$ for some $a_1, \dots, a_k \in A$, which means

$$\wp_B = X_{\top} = X_{a_1 \vee \dots \vee a_k} = X_{a_1} \cup \dots \cup X_{a_k}$$

with $X_{a_1}, \dots, X_{a_k} \in \mathcal{U}$, so we have found a finite subcover in \mathcal{U} .

$\top \notin J$: Then J is a proper ideal, so by Corollary 1.81 there exists a prime ideal K with $J \subseteq K$. But we cannot find $a \in A$ such that K equals X_a , so $K \in \wp_B$, but K fails to be covered by \mathcal{U} , which is a contradiction.

Thus (\wp_B, τ) is a compact space, which is sometimes called the *prime ideal space* of the Boolean algebra.

We conclude that the sets X_a are clopen, since $X_{-a} = \wp_B \setminus X_a$. Moreover, each clopen set in this space can be represented in this way. In fact, let U be clopen, thus $U = \bigcup \{X_a \mid a \in A\}$ for some $A \subseteq B$. Since U is closed, it is compact by Lemma 1.97, so there exist $a_1, \dots, a_n \in A$ such that $U = X_{a_1} \cup \dots \cup X_{a_n} = X_{a_1 \vee \dots \vee a_n}$. 

Compactness is formulated in terms of a cover through arbitrary open sets. Alexander's Theorem states that it is sufficient to consider covers which come from a subbase for the topology. This is usually quite a considerable help, since subbases are sometimes easier to handle than the connection of all open sets. The proof comes as an application of Zorn's Lemma. The proof follows essentially the one given for [HS65, Theorem 6.40].

Theorem 1.99 *Let (X, τ) be a topological space with a subbase \mathcal{S} . Then the following statements are equivalent.*

1. X is compact.
2. Each cover of X by elements of \mathcal{S} contains a finite subcover.

Proof Because the elements of a subbase are open, the implication $1 \Rightarrow 2$ is trivial, hence we have to show $2 \Rightarrow 1$. Assume that the assertion is false, and define

$$\mathfrak{Z} := \{\mathcal{C} \mid \mathcal{C} \text{ is an open cover of } X \text{ without a finite subcover}\}.$$

Order \mathfrak{Z} by inclusion, and let $\mathfrak{Z}_0 \subseteq \mathfrak{Z}$ be a chain, then $\mathcal{C} := \bigcup \mathfrak{Z}_0 \in \mathfrak{Z}$. In fact, it is clear that \mathcal{C} is a cover, and assume that \mathcal{C} has a finite subcover, say $\{E_1, \dots, E_k\}$. Then $E_j \in \mathcal{C}_j \in \mathfrak{Z}_0$, and since \mathfrak{Z}_0 is a chain with respect to inclusion, we find some $\mathcal{C}_i \in \mathfrak{Z}_0$ with $\{E_1, \dots, E_k\} \subseteq \mathcal{C}_i$, which is a contradiction. By Zorn's Lemma, \mathfrak{Z} has a maximal element \mathcal{V} . This means that

- \mathcal{V} is an open cover of X .
- \mathcal{V} does not contain a finite subcover.
- If $U \in \tau$ is open with $U \notin \mathcal{V}$, then $\mathcal{V} \cup \{U\}$ contains a finite subcover.

Let $\mathcal{W} := \mathcal{V} \cap \mathcal{S}$, hence all elements of \mathcal{V} which are taken from the subbase. By assumption, no finite subfamily of \mathcal{W} covers X , hence \mathcal{W} is not a cover for X , which implies that $R := X \setminus \bigcup \mathcal{W} \neq \emptyset$. Let $x \in R$, then there exists $V \in \mathcal{V}$ such that $x \in V$. Since V is open and \mathcal{S} is a subbase, we find $S_1, \dots, S_k \in \mathcal{S}$ with $x \in S_1 \cap \dots \cap S_k \subseteq V$. Because $x \notin \bigcup \mathcal{W}$, we conclude that no S_j is an element of \mathcal{V} (otherwise $S_j \in \mathcal{V} \cap \mathcal{S} = \mathcal{W}$, a contradiction). \mathcal{V} is maximal, each S_j is open, thus $\mathcal{V} \cup \{S_j\}$ contains a finite cover of X . Hence we can find for each j some open set A_j which is a finite union of elements in \mathcal{V} such that $A_j \cup S_j = X$. But this means

$$V \cup \bigcup_{j=1}^k A_j \supseteq \left(\bigcap_{j=1}^k S_j \right) \cup \left(\bigcup_{j=1}^k A_j \right) = X.$$

Hence X can be covered through a finite number of elements in \mathcal{V} ; this is a contradiction to the maximality of \mathcal{V} . \dashv

The Priestley topology as discussed by Goldblatt [Gol12] provides a first example for the use of Alexander's Theorem.

Example 1.100 Given $x \in X$, define

$$\begin{aligned} \|x\| &:= \{A \subseteq X \mid x \in A\}, \\ -\|x\| &:= \{A \subseteq X \mid x \notin A\}. \end{aligned}$$

The *Priestley topology* on $\mathcal{P}(X)$ is defined as the topology which is generated by the subbase

$$\mathcal{S} := \{\|x\| \mid x \in X\} \cup \{-\|x\| \mid x \in X\}.$$

Hence the basic sets of this topology have the form

$$\|x_1\| \cap \dots \cap \|x_k\| \cap -\|y_1\| \cap \dots \cap -\|y_n\|$$

for $x_1, \dots, x_k, y_1, \dots, y_n \in X$ and some $n, k \in \mathbb{N}$.

We claim that $\mathcal{P}(X)$ is compact in the Priestley topology. In fact, let \mathcal{C} be a cover of $\mathcal{P}(X)$ with elements from the subbase \mathcal{S} . Put $P := \{x \in X \mid -\|x\| \in \mathcal{C}\}$. Then $P \in \mathcal{P}(X)$, so we must find some element from \mathcal{C} which contains P . If $P \in -\|x\| \in \mathcal{C}$ for some $x \in X$, this means $x \notin P$, so by definition $-\|x\| \notin \mathcal{C}$, which is a contradiction. Thus there exists $x \in X$ such that $P \in \|x\| \in \mathcal{C}$. But this means $x \in P$, hence $-\|x\| \in \mathcal{C}$, so $\{\|x\|, -\|x\|\} \subseteq \mathcal{C}$ is a cover of $\mathcal{P}(X)$. This $\mathcal{P}(X)$ is compact by Alexander's Theorem 1.99. \mathfrak{M}

1.6 Boolean σ -Algebras

We generalize the notion of a Boolean algebra by introducing countable operations, leading to Boolean σ -algebras. This extension becomes important e.g., when working with probabilities or, more general, with measures. For example, one of the fundamental probability laws states

that the probability of a disjoint union of countable events equals the infinite sum of the events' probabilities. In order to express this adequately, the domain of the probability must be closed under countable unions.

We assume in this section that $(\mathbb{A}\mathbb{C})$ holds.

Given a Boolean algebra B , we associate with the lattice operations on B an order relation \leq by

$$a \leq b \iff a \wedge b = a \quad (\iff a \vee b = b).$$

We will switch in the discussion below between the order and the use of the algebraic operations.

Definition 1.101 *A Boolean algebra B is called a Boolean σ -algebra iff it is closed under countable suprema and infima.*

Example 1.102 The power set of each set is a Boolean σ -algebra. Consider

$$\mathcal{A} := \{A \subseteq \mathbb{R} \mid A \text{ is countable or } \mathbb{R} \setminus A \text{ is countable}\}.$$

Then \mathcal{A} is a Boolean σ -algebra (we use here that the countable union of countable set is countable again, hence $(\mathbb{A}\mathbb{C})$). This is sometimes called the *countable-cocountable σ -algebra*. On the other hand, her little sister,

$$\mathcal{D} := \{A \subseteq \mathbb{R} \mid A \text{ is finite or } \mathbb{R} \setminus A \text{ is finite}\},$$

the finite-cofinite algebra, is a Boolean algebra, but evidently no σ -algebra. \upharpoonright

If $(a_n)_{n \in \mathbb{N}}$ is an at most countable subset of the Boolean σ -algebra B , then we define

$$\begin{aligned} \bigwedge_{n \in \mathbb{N}} a_n &:= \inf\{a_n \mid n \in \mathbb{N}\}, \\ \bigvee_{n \in \mathbb{N}} a_n &:= \sup\{a_n \mid n \in \mathbb{N}\}. \end{aligned}$$

In addition, we note that

$$\begin{aligned} \inf \emptyset &= \top, \\ \sup \emptyset &= \perp. \end{aligned}$$

We know that a Boolean algebra is a distributive lattice, for a Boolean σ -algebra a stronger infinite distributive law holds.

Lemma 1.103 *Let B be a Boolean σ -algebra, $(a_n)_{n \in \mathbb{N}}$ be a sequence of elements in B , then*

$$\begin{aligned} b \wedge \bigvee_{n \in \mathbb{N}} a_n &= \bigvee_{n \in \mathbb{N}} (b \wedge a_n), \\ b \vee \bigwedge_{n \in \mathbb{N}} a_n &= \bigwedge_{n \in \mathbb{N}} (b \vee a_n) \end{aligned}$$

holds for any $b \in B$.

Proof We establish the first equality, the second one follows by duality. Since $b \wedge a_n \leq b$ and $b \wedge a_n \leq a_n$, we see that $\bigvee_{n \in \mathbb{N}} (b \wedge a_n) \geq b \wedge \bigvee_{n \in \mathbb{N}} a_n$. For establishing the reverse inequality, assume that s is an upper bound to $\{b \wedge a_n \mid n \in \mathbb{N}\}$, hence $b \wedge a_n \leq s$ for all $n \in \mathbb{N}$, consequently, $a_n = (b \wedge a_n) \vee (-b \wedge a_n) \leq s \vee (-b \wedge a_n) \leq s \vee -b$. Thus

$$b \wedge \bigvee_{n \in \mathbb{N}} a_n \leq b \wedge (s \vee -b) = (b \wedge s) \vee (b \wedge -b) \leq b \wedge s \leq s.$$

Hence s is an upper bound to $b \wedge \bigvee_{n \in \mathbb{N}} a_n$ as well. Now apply this to the upper bound $s := \bigvee_{n \in \mathbb{N}} (b \wedge a_n)$. \dashv

Let A be a non-empty subset of a Boolean σ -algebra B , then there exists a smallest σ -algebra C which contains A . In fact, this must be

$$C = \bigcap \{D \subseteq B \mid D \text{ is a } \sigma\text{-algebra with } A \subseteq D\}.$$

We first note that the intersection of a set of σ -algebras is a σ -algebra again. Moreover, there exists always a σ -algebra which contains A , viz., the superset B . Consequently, C the the object of our desire, it is denoted by $\sigma(A)$, so that $\sigma(A)$ denotes the smallest σ -algebra containing A . σ is an example for a *closure operator*: We have $A \subseteq \sigma(A)$, and $A_1 \subseteq A_2$ implies $\sigma(A_1) \subseteq \sigma(A_2)$, moreover, applying the operator twice does not yield anything new: $\sigma(\sigma(A)) = \sigma(A)$.

Example 1.104 Let $A := \{[a, b] \mid a, b \in [0, 1]\}$ be the set of all closed intervals $[a, b] := \{x \in \mathbb{R} \mid a \leq x \leq b\}$ of the unit interval $[0, 1]$. Denote by $B := \sigma(A)$ the σ -algebra generated by A ; the elements of B are sometimes called the *Borel sets* of $[0, 1]$. Then the half open intervals $[a, b[$ and $]a, b]$ are members of B . We can write, e.g., $[a, b[= \bigcup_{n \in \mathbb{N}} [a, b - 1/n]$. Since $[a, b - 1/n] \in A \subseteq B$ for all $n \in \mathbb{N}$, and since B is closed under countable unions, the claim follows.

A more complicated Borel set is constructed in this way: define $C_0 := [0, 1]$ and assume that C_n is defined already as a union of 2^n mutually disjoint intervals of length $1/3^n$ each, say $C_n = \bigcup_{1 \leq j \leq 2^n} I_j$. Obtain C_{n+1} by removing the open middle third of each interval I_j . For example

$$\begin{aligned} C_0 &= [0, 1], \\ C_1 &= [0, 1/3] \cup [2/3, 1], \\ C_2 &= [0, 1/9] \cup [2/9, 1/3] \cup [2/3, 7/9] \cup [8/9, 1], \\ C_3 &= [0, 1/27] \cup [2/27, 1/9] \cup [2/9, 7/27] \cup [8/27, 2/3] \cup [2/3, 19/27] \\ &\quad \cup [20/27, 7/9] \cup [8/9, 25/27] \cup [26/27, 1] \end{aligned}$$

and so on. Clearly $C_n \in B$, because this set is the finite union of closed intervals. Now put

$$C := \bigcap_{n \in \mathbb{N}} C_n,$$

then $C \in B$, because it is the countable intersection of sets in B . This set is known as the *Cantor ternary set*. ☞

The next two examples deal with σ -algebras of sets, each defined on the infinite product $\{0, 1\}^{\mathbb{N}}$. It may be used as a model for an infinite sequence of flipping coins — 0 denoting head, 1 denoting tail. But we can only observe a finite numbers of these events, probably as long as we want. So we cater for that by having a look at the σ -algebra which is defined by these finite observations.

Example 1.105 Let $X := \{0, 1\}^{\mathbb{N}}$ be the set of all infinite binary sequences, and put $\mathcal{B} := \sigma(\{A_{k,i} \mid k \in \mathbb{N}, i = 0, 1\})$ with $A_{k,i} := \{\langle x_1, x_2, \dots \rangle \mid x_k = i\}$ as the set of all sequences the k -th component of which is i .

We claim that that for $r \in \mathbb{N}_0$ both $S_{k,r} := \{\langle x_1, x_2, \dots \rangle \in X \mid x_1 + \dots + x_k = r\}$ and $T_r := \{\langle x_1, x_2, \dots \rangle \in X \mid \sum_{i=0}^{\infty} x_i = r\}$ are elements of \mathcal{B} .

In fact, given a finite binary sequence $v := \langle v_1, \dots, v_k \rangle$, the set

$$Q_v := \{x \in X \mid \langle x_1, \dots, x_k \rangle = v\} = \bigcap_{i=1}^k A_{i,v_i}$$

is a member of \mathcal{B} , the set $L_{k,r}$ of binary sequences of length k which sum up to r is finite. Thus

$$S_{k,r} = \bigcup_{v \in L_{k,r}} Q_v \in \mathcal{B}.$$

✎

We continue the example by looking at all sequences for which the average result of flipping a coin n times will converge as n tends to infinity.

Example 1.106 Let $X := \{0, 1\}^{\mathbb{N}}$ be the set of all infinite binary sequences as in Example 1.105, and put

$$W := \{\langle x_1, x_2, \dots \rangle \in X \mid \frac{1}{n} \sum_{i=1}^n x_i \text{ converges}\}.$$

We claim that $W \in \mathcal{B}$, noting that a real sequence $(y_n)_{n \in \mathbb{N}}$ converges iff it is a Cauchy sequence, i.e., iff given $0 < \epsilon \in \mathbb{Q}$ there exists $n_0 \in \mathbb{N}$ such that $|y_m - y_n| < \epsilon$ for all $n, m \geq n_0$.

Given $F \subseteq \mathbb{N}$ finite, the set

$$\begin{aligned} H_F &:= \{x \in X \mid x_j = 1 \text{ for all } j \in F \text{ and } x_i = 0 \text{ for all } i \notin F\} \\ &= \bigcap_{j \in F} A_{j,1} \cap \bigcap_{i \notin F} A_{i,0} \end{aligned}$$

is a member of \mathcal{B} ; since there are countably many finite subsets of \mathbb{N} which have exactly r elements, we obtain $T = \bigcup \{H_F \mid F \subseteq \mathbb{N} \text{ with } |F| = r\}$, which is a countable union of elements of \mathcal{B} , hence an element of \mathcal{B} .

The sequence $(\frac{1}{n} \sum_{i=1}^n x_i)_{n \in \mathbb{N}}$ converges iff

$$\forall \epsilon > 0, \epsilon \in \mathbb{Q} \exists n_0 \in \mathbb{N} \forall n \geq n_0 \forall m \geq n_0 : \left| \frac{1}{n} \sum_{i=1}^n x_i - \frac{1}{m} \sum_{i=1}^m x_i \right| < \epsilon,$$

thus iff

$$\langle x_1, x_2, \dots \rangle \in \bigcap_{\epsilon > 0, \epsilon \in \mathbb{Q}} \bigcup_{n_0 \in \mathbb{N}} \bigcap_{n \geq n_0} \bigcap_{m \geq n_0} W_{n, m, \epsilon}.$$

with

$$W_{n, m, \epsilon} := \{ \langle x_1, x_2, \dots \rangle \mid \left| \frac{1}{n} \sum_{i=1}^n x_i - \frac{1}{m} \sum_{i=1}^m x_i \right| < \epsilon \}.$$

Now $\langle x_1, x_2, \dots \rangle \in W_{n, m, \epsilon}$ iff $|m \cdot \sum_{i=1}^n x_i - n \cdot \sum_{j=1}^m x_j| < n \cdot m \cdot \epsilon$. If $n < m$, this is equivalent to

$$-n \cdot m \cdot \epsilon < (m - n) \cdot \sum_{i=1}^n x_i - n \cdot \sum_{j=n+1}^m x_j < n \cdot m \cdot \epsilon$$

hence $-n \cdot m \cdot \epsilon < (m - n) \cdot a - n \cdot b < n \cdot m \cdot \epsilon$ for $a = \sum_{i=1}^n x_i$ and $b = \sum_{j=n+1}^m x_j$; the same applies to the case $m < n$. Since there are only finitely many combinations of $\langle a, b \rangle$ satisfying these constraints, we conclude that $W_{n, m, \epsilon} \in \mathcal{B}$, so that the set W of all sequences for which the average sum converges is a member of \mathcal{B} as well. \mathbb{M}

1.6.1 Construction Through Transfinite Induction

The description of $\sigma(A)$ given above is non-constructive; it is done through a closure operation, from the outside, so to speak. Transfinite induction permits us to construct $\sigma(A)$. In order to describe it, we introduce two operators on the subsets of B as follows. Let $H \subseteq B$, then

$$H_\sigma := \left\{ \bigvee_{n \in \mathbb{N}} a_n \mid a_n \in H \text{ for all } n \in \mathbb{N} \right\},$$

$$H_\delta := \left\{ \bigwedge_{n \in \mathbb{N}} a_n \mid a_n \in H \text{ for all } n \in \mathbb{N} \right\}.$$

Thus H_σ contains all countable suprema of elements of H , and H_δ contains all countable infima. Hence A is a Boolean sub σ -algebra of B iff

$$A_\sigma \subseteq A, A_\delta \subseteq A, \text{ and } \{-a \mid a \in A\} \subseteq A$$

hold.

So couldn't we, when constructing $\sigma(A)$, just take all complements, then all countable infima and suprema of elements in A , and then their countable suprema and infima, and so on? This is the basic idea for the construction. But since the process indicated above is not guaranteed to terminate after a finite number of applications of the σ -and the δ -operations, we do a transfinite construction.

So fix $A \subseteq B$, and define by transfinite induction

$$A_0 := A \cup \{-a \mid a \in A\},$$

$$A_\zeta := \bigcup_{\eta < \zeta} A_\eta, \text{ if } \zeta \text{ is a limit ordinal}$$

$$A_{\zeta+1} := (A_\zeta)_\sigma, \text{ if } \zeta \text{ is odd,}$$

$$A_{\zeta+1} := (A_\zeta)_\delta, \text{ if } \zeta \text{ is even,}$$

$$A_\omega := \bigcup_{\zeta < \omega} A_\zeta.$$

It is clear that $A_\zeta \subseteq C$ holds for each σ -algebra C which contains A , so that $A_\omega \subseteq \sigma(A)$ is inferred.

Let us work on the other inclusion. It is sufficient to show that A_ω is a σ -algebra. This is so because $A \subseteq A_\omega$, so that in this case A_ω would contribute to the intersections defining $\sigma(A)$, hence we could infer $A_\omega \subseteq \sigma(A)$. We prove the assertion through a series of auxiliary statements, noting that $\langle A_\zeta \mid \zeta < \omega \rangle$ forms a chain with respect to set inclusion.

Lemma 1.107 *For each $\zeta < \omega$, if $a \in A_\zeta$, then $-a \in A_{\zeta+1}$.*

Proof The proof proceeds by transfinite induction. The assertion is true for $\zeta = 0$; assume that it is true for all $\eta < \zeta$.

If ζ is a limit ordinal, we know that we can find for $a \in A_\zeta$ an ordinal $\eta < \zeta$ with $a \in A_\eta$, hence by induction hypothesis $-a \in A_{\eta+1} \subseteq A_\zeta$, because $\eta+1 < \zeta$ by the definition of a limit ordinal (see Definition 1.29 on page 16).

If ζ is even, but not a limit ordinal, we can write ζ as $\zeta = \xi + 1$. Then $A_\zeta = (A_\xi)_\sigma$, hence $a = \bigvee_{n \in \mathbb{N}} a_n$ for some $a_n \in A_\xi \subseteq A_\zeta$, so that $-a = \bigwedge_{n \in \mathbb{N}} (-a_n) \in (A_\xi)_\delta = A_{\zeta+1}$. The argumentation for ζ odd is exactly the same. \dashv

Thus A_ω is closed under complementation. Closure under countable infima and suprema is shown similarly, but we have to cater somehow for a countable sequence of countable ordinals.

Lemma 1.108 *A_ω is closed under countable infima and countable suprema.*

Proof We focus on countable suprema, the proof for infima works exactly in the same way. Let $(a_n)_{n \in \mathbb{N}}$ be a sequence of elements in A_ω , then we find ordinal numbers $\zeta_n < \omega$ such that $a_n \in A_{\zeta_n}$. Because ζ_n is countable for each $n \in \mathbb{N}$, we conclude from Proposition 1.38 that $\zeta^* := \bigcup_{n \in \mathbb{N}} \zeta_n$ is a countable ordinal, so that $\zeta^* < \omega$. Because $\langle A_\zeta \mid \zeta < \omega \rangle$ forms a chain, we infer that $a_n \in A_{\zeta^*}$ for all $n \in \mathbb{N}$. Consequently, $\bigvee_{n \in \mathbb{N}} a_n \in (A_{\zeta^*})_\sigma \subseteq A_\omega$. \dashv

Thus we have shown

Proposition 1.109 $A_\omega = \sigma(A)$. \dashv

1.6.2 Factoring Through σ -Ideals

Factoring a Boolean σ -algebra through an ideal works as for general Boolean algebras, resulting in a Boolean algebra again. There is no reason why the factor algebra should be a σ -algebra, however, so if we want to obtain a σ -algebra we have to make stronger assumptions on the object used for factoring.

Definition 1.110 *Let B be a Boolean algebra, $I \subseteq B$ an ideal. I is called a σ -ideal iff $\sup_{n \in \mathbb{N}} a_n \in I$, provided $a_n \in I$ for all $n \in \mathbb{N}$.*

Not every ideal is a σ -ideal: $\{F \subseteq \mathbb{N} \mid F \text{ is finite}\}$ is an ideal but certainly not a σ -ideal in $\mathcal{P}(\mathbb{N})$, even if $\mathcal{P}(\mathbb{N})$ is a Boolean σ -algebra.

The following statement is the σ -variant of Proposition 1.84.

Proposition 1.111 *Let B be a Boolean σ -algebra and $I \subseteq B$ be a σ -ideal. Then B/I is a Boolean σ -algebra.*

Proof 1. Because each Boolean σ -algebra is a Boolean algebra, and each σ -ideal is an ideal, we may conclude from Proposition 1.84 that B/I is a Boolean algebra. Hence it remains to be shown that this Boolean algebra is closed under countable suprema; since B/I is closed under complementation, closedness under countable infima will follow.

2. Let $a_n \in B$, then $a := \bigvee_{n \in \mathbb{N}} a_n \in B$. We claim that $[a]_{\sim_I} = \bigvee_{n \in \mathbb{N}} [a_n]_{\sim_I}$. Because $a_n \leq a$ for all $n \in \mathbb{N}$, we conclude that $[a_n]_{\sim_I} \leq [a]_{\sim_I}$ for all $n \in \mathbb{N}$, hence $\bigvee_{n \in \mathbb{N}} [a_n]_{\sim_I} \leq [a]_{\sim_I}$. Now let $[a_n]_{\sim_I} \leq [b]_{\sim_I}$ for all $n \in \mathbb{N}$, then we show that $[a]_{\sim_I} \leq [b]_{\sim_I}$. In fact, because $[a_n]_{\sim_I} \leq [b]_{\sim_I}$ we conclude that $c_n := a_n \ominus (a_n \wedge b) \in I$ and $b \wedge c_n = \perp$ for all $n \in \mathbb{N}$ (since $c_n = a_n \wedge \neg(a_n \wedge b)$). Thus $a_n = c_n \vee (a_n \wedge b)$, so that we have $\bigvee_{n \in \mathbb{N}} a_n = (a \wedge b) \vee \bigvee_{n \in \mathbb{N}} c_n$ by the infinite distributive law from Lemma 1.103. This implies $a \ominus (a \wedge b) = \bigvee_{n \in \mathbb{N}} c_n \in I$, or, equivalently, $[a]_{\sim_I} \leq [b]_{\sim_I}$. Consequently, $[a]_{\sim_I}$ is the smallest upper bound to $\{[a_n]_{\sim_I} \mid n \in \mathbb{N}\}$. \dashv

1.6.3 Measures

Boolean σ -algebras model events. The top element \top is interpreted as an event which can happen unconditionally and always, the bottom element \perp is the impossible event. The complement of an event is an event, and if we have a countable sequence of events, then their supremum is an event, viz., the event that at least one of the event in the sequence happens.

To illustrate, suppose that we have a set T of traders which may form unions or coalitions, then T as well as \emptyset are coalitions; if A is a coalition, then $T \setminus A$ is a coalition as well, and if A_n is a coalition for each $n \in \mathbb{N}$, then we want to be able to form the “big” coalition $\bigcup_{n \in \mathbb{N}} A_n$. Hence the set of all coalitions forms a σ -algebra.

We deal in the sequel with set based σ -algebras, so we fix a set S of events.

Definition 1.112 *Let $\mathcal{C} \subseteq \mathcal{P}(S)$ be a family of sets with $\emptyset \in \mathcal{C}$. A map $\mu : \mathcal{C} \rightarrow [0, \infty]$ with $\mu(\emptyset) = 0$ is called*

1. *monotone iff $\mu(A) \leq \mu(B)$ for $A, B \in \mathcal{C}, A \subseteq B$,*
2. *additive iff $\mu(A \cup B) = \mu(A) + \mu(B)$ for all $A, B \in \mathcal{C}$, with $A \cup B \in \mathcal{C}$ and $A \cap B = \emptyset$,*
3. *countably subadditive iff $\mu(\bigcup_{n \in \mathbb{N}} A_n) \leq \sum_{n \in \mathbb{N}} \mu(A_n)$, whenever $(A_n)_{n \in \mathbb{N}}$ is a sequence of sets in \mathcal{C} with $\bigcup_{n \in \mathbb{N}} A_n \in \mathcal{C}$,*
4. *countably additive iff $\mu(\bigcup_{n \in \mathbb{N}} A_n) = \sum_{n \in \mathbb{N}} \mu(A_n)$, whenever $(A_n)_{n \in \mathbb{N}}$ is a mutually disjoint sequence of sets in \mathcal{C} with $\bigcup_{n \in \mathbb{N}} A_n \in \mathcal{C}$,*

If \mathcal{C} is a σ -algebra, then a map $\mu : \mathcal{C} \rightarrow [0, \infty]$ with $\mu(\emptyset) = 0$ is called a measure iff μ is monotone and countably additive.

Note that we permit that μ assumes the value $+\infty$. Clearly, a countably additive set function is additive, and it is countably subadditive, provided it is monotone.

Example 1.113 Let S be a set, and define for $a \in S, A \subseteq S$

$$\delta_a(A) := \begin{cases} 1, & \text{if } a \in A \\ 0, & \text{otherwise.} \end{cases}$$

Then δ_a is a measure on the power set of S . It is usually referred to as the *Dirac measure* on a . \mathfrak{M}

A slightly more complicated example indicates the connection to ultrafilters.

Example 1.114 Let $\mu : \mathcal{P}(S) \rightarrow \{0, 1\}$ be a binary valued measure. Define

$$\mathcal{F} := \{A \subseteq S \mid \mu(A) = 1\}$$

Then \mathcal{F} is an ultrafilter on $\mathcal{P}(S)$. First, we check that \mathcal{F} is a filter: $\emptyset \notin \mathcal{F}$ is obvious, and if $A \in \mathcal{F}$ with $A \subseteq B$, then certainly $B \in \mathcal{F}$. Let $A, B \in \mathcal{F}$, then $2 = \mu(A) + \mu(B) = \mu(A \cup B) + \mu(A \cap B)$, hence $\mu(A \cap B) = 1$, thus $A \cap B \in \mathcal{F}$. Thus \mathcal{F} is indeed a filter. It is also an ultrafilter by Lemma 1.63, because $A \notin \mathcal{F}$ implies $S \setminus A \in \mathcal{F}$.

The converse construction, viz., to generate a binary valued measure from a filter, would require $\bigcup_{n \in \mathbb{N}} A_n \in \mathcal{F}$ if and only if there exists $n \in \mathbb{N}$ with $A_n \in \mathcal{F}$ for any disjoint family $(A_n)_{n \in \mathbb{N}}$. This, however, leads to very deep questions on Set Theory, see [Jec06, Chapter 10] for a discussion. \mathfrak{M}

Let us have a look at an important example.

Example 1.115 Let $\mathcal{C} := \{[a, b] \mid a, b \in [0, 1]\}$ be all left open, right closed intervals of the unit interval. Put $\ell([a, b]) := b - a$, hence $\ell(I)$ is the length of interval I . Note that $\ell(\emptyset) = \ell([a, a]) = 0$. Certainly $\ell : \mathcal{C} \rightarrow \mathbb{R}_+$ is monotone and additive.

1. If $\bigcup_{i=1}^k [a_i, b_i] \subseteq [a, b]$, and the intervals are disjoint, then $\sum_{i=1}^k \ell([a_i, b_i]) \leq \ell([a, b])$. The proof proceeds by induction on the number k of intervals. For the induction step we have mutually disjoint intervals with $\bigcup_{i=1}^{k+1} [a_i, b_i] \subseteq [a, b]$. Renumbering, if necessary, we may assume that $a_1 \leq b_1 \leq a_2 \leq b_2 \leq \dots \leq a_k \leq b_k \leq a_{k+1} \leq b_{k+1}$. Then $\sum_{i=1}^k \ell([a_i, b_i]) + \ell([a_{k+1}, b_{k+1}]) \leq \ell([a_1, b_k]) + \ell([a_{k+1}, b_{k+1}]) \leq \ell([a, b])$, because ℓ is monotone and additive.
2. If $\bigcup_{i=1}^\infty [a_i, b_i] \subseteq [a, b]$, and the intervals are disjoint, then $\sum_{i=1}^k \ell([a_i, b_i]) \leq \ell([a, b])$ for all k , hence

$$\sum_{i=1}^\infty \ell([a_i, b_i]) = \sup_{k \in \mathbb{N}} \sum_{i=1}^k \ell([a_i, b_i]) \leq \ell([a, b]).$$

3. If $[a, b] \subseteq \bigcup_{i=1}^k [a_i, b_i]$ then $\ell([a, b]) \leq \sum_{i=1}^k \ell([a_i, b_i])$ with not necessarily disjoint intervals. This is established by induction on k . If $k = 1$, the assertion is obvious. The induction step proceeds as follows: Assume that $[a, b] \subseteq \bigcup_{i=1}^{k+1} [a_i, b_i]$. By renumbering, if necessary, we can assume that $a_{k+1} < b \leq b_{k+1}$. If $a_{k+1} \leq a$, the assertion follows, so let us assume that $a < a_{k+1}$. Then $[a, a_{k+1}] \subseteq \bigcup_{i=1}^k [a_i, b_i]$, so that by the induction hypothesis $a_{k+1} - a = \ell([a, a_{k+1}]) \leq \sum_{i=1}^k \ell([a_i, b_i])$. Thus

$$\ell([b, a]) = b - a \leq (a_{k+1} - a) + (b_{k+1} - a_{k+1}) \leq \sum_{i=1}^{k+1} \ell([a_i, b_i]).$$

4. Now assume that $]a, b] \subseteq \bigcup_{i=1}^{\infty}]a_i, b_i]$. This is a little bit more complicated since we do not know whether the interval $]a, b]$ is covered already by a finite number of intervals, so we have to resort to a little trick. The interval $[a + \epsilon, b]$ is closed and bounded, hence compact, for every fixed $\epsilon > 0$; we also know that for each $i \in \mathbb{N}$ the semi-open interval $]a_i, b_i]$ is contained in the open interval $]a_i, b_i + \epsilon/2^i[$, so that we have

$$[a + \epsilon, b] \subseteq \bigcup_{i=1}^{\infty}]a_i, b_i + \epsilon/2^i[$$

By the Heine-Borel Theorem 1.88 we can find a finite subset of these intervals which cover $[a + \epsilon, b]$, say $[a + \epsilon, b] \subseteq \bigcup_{i \in K}]a_i, b_i + \epsilon/2^i[$, with $K \subseteq \mathbb{N}$ finite. Hence

$$]a + \epsilon, b] \subseteq \bigcup_{i \in K}]a_i, b_i + \epsilon/2^i],$$

and we conclude from the finite case that

$$b - (a + \epsilon) = \ell([a + \epsilon, b]) \leq \sum_{i \in K} \ell([a_i, b_i + \epsilon/2^i]) = \sum_{i=1}^{\infty} (b_i + \epsilon/2^i - a_i) < \sum_{i=1}^{\infty} \ell([a_i, b_i]) + \epsilon.$$

Since $\epsilon > 0$ was arbitrary, we have established

$$\ell([a, b]) \leq \sum_{i=1}^{\infty} \ell([a_i, b_i]).$$



Thus we have shown

Proposition 1.116 *Let \mathcal{C} be the set of all left open, right closed intervals of the unit interval, and denote by $\ell([a, b]) := b - a$ the length of interval $]a, b] \in \mathcal{C}$. Then $\ell : \mathcal{C} \rightarrow \mathbb{R}_+$ is monotone and countably additive. \dashv*

When having a look at \mathcal{C} we note that this family is not closed under complementation, but the complement of a set in \mathcal{C} can be represented through elements of \mathcal{C} , e.g., $]0, 1] \setminus]1/3, 1/2] =]0, 1/3] \cup]1/2, 1]$. This is captured through the following definition.

Definition 1.117 $\mathcal{R} \subseteq \mathcal{P}(S)$ is called a *semiring* iff

1. $\emptyset \in \mathcal{R}$,
2. \mathcal{R} is closed under finite intersections,
3. If $B \in \mathcal{R}$, then there exists a finite family $C_1, \dots, C_k \in \mathcal{R}$ with $S \setminus B = C_1 \cup \dots \cup C_k$.

Thus the complement of a set in \mathcal{R} can be represented through a finite disjoint union of elements of \mathcal{R} .

We want to extend $\ell : \mathcal{C} \rightarrow \mathbb{R}_+$ from the semiring of left open, right closed intervals to a measure λ on the σ -algebra $\sigma(\mathcal{C})$. This measure is fairly important, it is called the *Lebesgue measure* on the unit interval.

A first step towards an extension of ℓ to the σ -algebra generated by the intervals is the extension to the algebra generated by them. This can be accomplished easily once this algebra has been identified.

Lemma 1.118 *Let \mathcal{C} be the set of all left open, right closed intervals in $]0, 1]$. Then the algebra generated by \mathcal{C} consists of all disjoint unions of elements of \mathcal{C} .*

Proof Denote by

$$\mathcal{D} := \left\{ \bigcup_{1 \leq i \leq n}]a_i, b_i] \mid n \in \mathbb{N}, a_1 \leq b_1 \leq a_2 \leq b_2 \leq \dots \leq a_n \leq b_n \right\}$$

Then all elements of \mathcal{D} are certainly contained in the algebra generated by \mathcal{C} . If we can show that \mathcal{D} is an algebra itself, we are done, because then \mathcal{D} is the smallest algebra containing \mathcal{C} .

\mathcal{D} is certainly closed under finite unions and finite intersections, and $\emptyset \in \mathcal{D}$. The complement of $\bigcup_{1 \leq i \leq n}]a_i, b_i]$ is $]0, a_1] \cup]b_1, a_2] \cup \dots \cup]b_n, 1]$, which is a member of \mathcal{D} as well. Thus \mathcal{D} is also closed under complementation, hence is an algebra. \dashv

This permit us to extend ℓ to the algebra generated by the intervals:

Corollary 1.119 *ℓ extends uniquely to the algebra generated by \mathcal{C} such that the extension is monotone and countably additive.*

Proof Put

$$\ell\left(\bigcup_{1 \leq i \leq n}]a_i, b_i]\right) := \sum_{i=1}^n \ell([a_i, b_i]),$$

whenever $]a_i, b_i] \in \mathcal{C}$. This is well defined. Assume

$$\bigcup_{1 \leq i \leq n}]a_i, b_i] = \bigcup_{1 \leq j \leq m}]c_j, d_j],$$

then $]a_i, b_i]$ can be represented as a disjoint union of those intervals $]c_j, d_j]$ which it contains, so that we have

$$\begin{aligned} \sum_{i=1}^n \ell([a_i, b_i]) &= \sum_{i=1}^n \sum_{j=1}^m \ell([a_i, b_i] \cap]c_j, d_j]) \\ &= \sum_{j=1}^m \sum_{i=1}^n \ell([c_j, d_j] \cap]a_i, b_i]) \\ &= \sum_{j=1}^m \ell([c_j, d_j]) \end{aligned}$$

We may conclude from Example 1.115 that ℓ is countably additive on the algebra. \dashv

For the sake of illustration, let us assume that we have Lebesgue measure constructed already, and let us compute $\lambda(C)$ where C is the Cantor ternary set constructed in Example 1.104 on page 45. The construction of the ternary set is done through sets C_n , each of which is the union of 2^n mutually disjoint intervals of length $1/3^n$. If I is an interval of length 3^{-n} , we know that $\lambda(I) = 3^{-n}$, so that $\lambda(C_n) = (2/3)^n$. We also know that $C_1 \supseteq C_2 \supseteq \dots$, so that we have a descending chain of sets with $C = \bigcap_{n \in \mathbb{N}} C_n$.

In order to compute $\lambda(C)$, we need so know something about the behavior of measures when monotone limits of sets are encountered.

Lemma 1.120 *Let $\mu : \mathcal{A} \rightarrow [0, \infty]$ be a measure on the σ -algebra \mathcal{A} .*

1. *If $A_n \in \mathcal{A}$ is a monotone increasing sequence of sets in \mathcal{A} , and $A = \bigcup_{n \in \mathbb{N}} A_n$, then $\mu(A) = \sup_{n \in \mathbb{N}} \mu(A_n)$.*
2. *If $A_n \in \mathcal{A}$ is a monotone decreasing sequence of sets in \mathcal{A} , and $A = \bigcap_{n \in \mathbb{N}} A_n$, then $\mu(A) = \inf_{n \in \mathbb{N}} \mu(A_n)$, provided $\mu(A_k) < \infty$ for some $k \in \mathbb{N}$.*

Proof

1. We can write $A_n = \bigcup_{i=1}^n B_i$ with $B_1 := A_1$ and $B_i := A_i \setminus A_{i-1}$. Because the A_n form an increasing sequence, the B_i are mutually disjoint. Assume without loss of generality that $\mu(A_n) < \infty$ for all $n \in \mathbb{N}$ (otherwise the assertion is trivial), then by countable additivity and through telescoping

$$\mu(A) = \sum_{i=1}^{\infty} \mu(B_i) = \mu(A_1) + \sum_{i=1}^{\infty} (\mu(A_{i+1}) - \mu(A_i)) = \lim_{n \rightarrow \infty} \mu(A_n) = \sup_{n \in \mathbb{N}} \mu(A_n).$$

2. Assume $\mu(A_1) < \infty$, then the sequence $A_1 \setminus A_n$ is increasing towards $A_1 \setminus A$, hence

$$\mu(A) = \mu(A_1) - \mu(A_1 \setminus A) = \mu(A_1) - \sup_{n \in \mathbb{N}} \mu(A_1 \setminus A_n) = \inf_{n \in \mathbb{N}} \mu(A_n).$$

+

Ok, so let us return to the discussion of Cantor's set. We know that $\lambda(C_n) = (2/3)^n$, and that $C_1 \supseteq C_2 \supseteq C_3 \dots$, so we conclude

$$\lambda(C) = \inf_{n \in \mathbb{N}} \lambda(C_n) = 0.$$

So we have identified a geometrically fairly complicated set which has measure zero. This set is geometrically not easy to visualize, since it does not contain an interval of positive length.

Now fix a semiring $\mathcal{C} \subseteq \mathcal{P}(S)$ and $\mu : \mathcal{C} \rightarrow [0, \infty]$ with $\mu(\emptyset) = 0$, which is monotone and countably subadditive. We will first compute an outer approximation for each subset of S by elements of \mathcal{C} . But since the subsets of S may be as a whole somewhat inaccessible, and since \mathcal{C} may be somewhat small, we try to cover the subsets of S by countable unions of elements of \mathcal{C} and take the best approximation we can, i.e., we take the infimum. Define

$$\mu^*(A) := \inf \left\{ \sum_{n \in \mathbb{N}} \mu(C_n) \mid A \subseteq \bigcup_{n \in \mathbb{N}} C_n, C_n \in \mathcal{C} \right\}$$

for $A \subseteq S$. This is the *outer measure* of A associated with μ .

These are some interesting (for us, that is) properties of μ^* .

Lemma 1.121 *$\mu^* : \mathcal{P}(S) \rightarrow [0, \infty]$ is monotone and countably subadditive, $\mu^*(\emptyset) = 0$. If $A \in \mathcal{C}$, then $\mu^*(A) = \mu(A)$.*

Proof 1. Let $(A_n)_{n \in \mathbb{N}}$ be a sequence of subset of S , put $A := \bigcup_{n \in \mathbb{N}} A_n$. If $\sum_{n \in \mathbb{N}} \mu^*(A_n) < \infty$, we find for A_n a cover $\{C_{n,m} \mid m \in \mathbb{N}\} \subseteq \mathcal{C}$ with $\mu(A_n) \leq \sum_{m \in \mathbb{N}} \mu(C_{n,m}) \leq \mu^*(A_n) + \epsilon/2^n$,

thus $\{C_{n,m} \mid n, m \in \mathbb{N}\} \subseteq \mathcal{C}$ is a cover of A with $\mu(A) \leq \sum_{n,m \in \mathbb{N}} \mu(C_{n,m}) \leq \sum_{n \in \mathbb{N}} \mu(A_n) + \epsilon$. Since $\epsilon > 0$ was arbitrary, we conclude $\mu^*(A) \leq \sum_{n \in \mathbb{N}} \mu^*(A_n)$. If, however, $\sum_{n \in \mathbb{N}} \mu^*(A_n) = \infty$, the assertion is immediate.

2. The other properties are readily seen. \dashv

The next step is somewhat mysterious — it has been suggested by Carathéodory around 1914 for the construction of a measure extension. It splits a set $A = (A \cap X) \cup (A \cap S \setminus X)$ along an arbitrary other set X , and looks what happens to the outer measure. If $\mu^*(A) = \mu^*(A \cap X) + \mu^*(A \cap S \setminus X)$, then A is considered well behaved. Those sets which are well behaved no matter what set X we use for splitting are considered next.

Definition 1.122 *A set $A \subseteq S$ is called μ -measurable iff $\mu^*(X) = \mu^*(X \cap A) + \mu^*(X \cap S \setminus A)$ holds for all $X \subseteq S$. The set of all μ -measurable sets is denoted by \mathcal{C}_μ*

So take a μ -measurable set A and an arbitrary subset $X \subseteq S$, then X splits into a part $X \cap A$ which belongs to A and another one $X \cap S \setminus A$ which does not belong to A . Measuring these pieces through μ^* , we demand that they add up to $\mu^*(X)$ again.

These properties are immediate:

Lemma 1.123 *The outer measure has these properties*

1. $\mu^*(\emptyset) = 0$.
2. $\mu^*(A) \geq 0$ for all $A \subseteq S$.
3. μ^* is monotone.
4. μ^* is countably subadditive.

Proof We establish only the last property. Here we have to show that $\mu^*(\bigcup_{n \in \mathbb{N}} A_n) \leq \sum_{n \in \mathbb{N}} \mu^*(A_n)$. We may and do assume that all $\mu^*(A_n)$ are finite. Given $\epsilon > 0$ we find for each $n \in \mathbb{N}$ a sequence $B_{n,k} \in \mathcal{C}$ for A_n such that $A_n \subseteq \bigcup_{k \in \mathbb{N}} B_{n,k}$ and $\sum_{k \in \mathbb{N}} \mu(B_{n,k}) \leq \mu^*(A_n) + \epsilon/2^n$. Thus $\sum_{n,k \in \mathbb{N}} \mu(B_{n,k}) \leq \sum_{n \in \mathbb{N}} (\mu^*(A_n) + \epsilon/2^n) < \sum_{n \in \mathbb{N}} \mu^*(A_n) + \epsilon$, which implies $\sum_{n \in \mathbb{N}} \mu^*(A_n) \leq \mu^*(\bigcup_{n \in \mathbb{N}} A_n)$, because $\bigcup_{n \in \mathbb{N}} A_n \subseteq \bigcup_{n,k \in \mathbb{N}} B_{n,k}$, and because $\epsilon > 0$ was arbitrary. \dashv

Because countably subadditivity, we conclude

Corollary 1.124 *$A \in \mathcal{C}_\mu$ iff $\mu^*(X \cap A) + \mu^*(X \cap S \setminus A) \leq \mu^*(X)$ for all $X \subseteq S$. \dashv*

Let us have a look at the set of all μ -measurable sets. It turns out that the originally given sets are all μ -measurable, and that \mathcal{C}_μ is an algebra.

Proposition 1.125 *\mathcal{C}_μ is an algebra. Also if μ is additive, $\mathcal{C} \subseteq \mathcal{C}_\mu$ and $\mu(A) = \mu^*(A)$ for all $A \in \mathcal{C}$.*

Proof 1. \mathcal{C}_μ is closed under complementation; this is obvious from its definition, and $S \in \mathcal{C}_\mu$ is also clear. So we have only to show that \mathcal{C}_μ is closed under finite intersections. For simplicity, denote complementation by \cdot^c .

Now let $A, B \in \mathcal{C}_\mu$, we want to show

$$\mu^*(X) \geq \mu^*((A \cap B) \cap X) + \mu^*((A \cap B)^c \cap X),$$

for each $X \subseteq S$; from Corollary 1.124 we infer that this implies $A \cap B \in \mathcal{C}_\mu$. Since $B \in \mathcal{C}_\mu$ and then $A \in \mathcal{C}_\mu$, we know

$$\begin{aligned} \mu^*(X) &= \mu^*(X \cap B) + \mu^*(X \cap B^c) \\ &= \mu^*(X \cap (A \cap B)) + \mu^*(X \cap (A^c \cap B)) + \mu^*(X \cap (A \cap B^c)) + \mu^*(X \cap (A^c \cap B^c)) \\ &\geq \mu^*(X \cap (A \cap B)) + \mu^*(X \cap ((A^c \cap B) \cup (A \cap B^c) \cup (A^c \cap B^c))) \\ &\stackrel{(\ddagger)}{=} \mu^*(X \cap (A \cap B)) + \mu^*(X \cap (A \cap B)^c). \end{aligned}$$

Equality (\ddagger) uses

$$\begin{aligned} (A^c \cap B) \cup (A \cap B^c) \cup (A^c \cap B^c) &= (A^c \cap (B \cup B^c)) \cup (A \cap B^c) \\ &= A^c \cup (A \cap B^c) \\ &= A^c \cup B^c. \end{aligned}$$

Hence we see that $A \cap B$ satisfies the defining inequality.

2. We still have to show that $\mathcal{C} \subseteq \mathcal{C}_\mu$, and that μ^* extends μ . Let $A \in \mathcal{C}$, then $S \setminus A = D_1 \cup \dots \cup D_k$ for some disjoint $D_1, \dots, D_k \in \mathcal{C}$, because \mathcal{C} is a semiring. Fix $X \subseteq S$, and assume that $\mu^*(S) < \infty$ (otherwise, the assertion is trivial). Given $\epsilon > 0$ there exists in \mathcal{C} a cover $(A_n)_{n \in \mathbb{N}}$ of X with $\mu^*(X) < \sum_{n \in \mathbb{N}} \mu(A_n) + \epsilon$. Now put $B_n := A \cap A_n$ and $C_{i,n} := A_n \cap D_i$. Then $X \cap A \subseteq \bigcup_{n \in \mathbb{N}} B_n$ with $B_n \in \mathcal{C}$ and $X \cap A^c \subseteq \bigcup_{n \in \mathbb{N}, 1 \leq i \leq k} C_{i,n}$ with $C_{i,n} \in \mathcal{C}$. Hence

$$\begin{aligned} \mu^*(X \cap A) + \mu^*(X \cap A^c) &\leq \sum_{n \in \mathbb{N}} \mu(B_n) + \sum_{n \in \mathbb{N}, 1 \leq i \leq k} \mu(C_{i,n}) \\ &\leq \sum_{n \in \mathbb{N}} \mu(A_n) \\ &< \mu^*(X) + \epsilon, \end{aligned}$$

because μ is (finitely) additive. Hence $A \in \mathcal{C}_\mu$. μ^* is an extension to μ by Lemma 1.121. \dashv

But we can in fact say more on the behavior of μ^* on \mathcal{C}_μ : It turns out to be additive on the splitting parts.

Lemma 1.126 *Let $\mathcal{D} \subseteq \mathcal{C}_\mu$ be a finite or infinite family of mutually disjoint sets in \mathcal{C}_μ , then*

$$\mu^*(X \cap \bigcup_{D \in \mathcal{D}} D) = \sum_{D \in \mathcal{D}} \mu^*(X \cap D)$$

holds for all $X \subseteq S$.

Proof 1. We establish the equality above for finite \mathcal{D} , say, $\mathcal{D} = \{A_1, \dots, A_n\}$ with $A_n \in \mathcal{C}_\mu$ for $1 \leq j \leq n$. From this we obtain that the equality holds in the countable case as well, because then

$$\mu^*(X \cap \bigcup_{i=1}^{\infty} A_i) \geq \mu^*(X \cap \bigcup_{i=1}^n A_i) = \sum_{i=1}^n \mu^*(X \cap A_i),$$

for all $n \in \mathbb{N}$, so that $\mu^*(X \cap \bigcup_{i=1}^{\infty} A_i) \geq \sum_{i=1}^{\infty} \mu^*(X \cap A_i)$, which together with countable subadditivity gives the desired result.

2. The proof for $\mu^*(X \cap \bigcup_{i=1}^n A_i) = \sum_{i=1}^n \mu^*(X \cap A_i)$ proceeds by induction on n , starting with $n = 2$. If $A_1 \cup A_2 = S$, this is just the definition that A_1 (or A_2) is μ -measurable, so the equality holds. If $A_1 \cup A_2 \neq S$, we note that $\mu^*(X) = \mu^*((X \cap (A_1 \cup A_2)) \cap A_1) + \mu^*((X \cap (A_1 \cup A_2)) \cap S \setminus A_1)$. Evaluating the pieces, we see that

$$\begin{aligned} (X \cap (A_1 \cup A_2)) \cap A_1 &= X \cap A_1, \\ (X \cap (A_1 \cup A_2)) \cap S \setminus A_1 &= X \cap A_2, \end{aligned}$$

because $A_1 \cap A_2 = \emptyset$. The induction step is straightforward:

$$\begin{aligned} \mu^*(X \cap \bigcup_{i=1}^{n+1} A_i) &= \mu^*((X \cap \bigcup_{i=1}^n A_i) \cup (X \cap A_{n+1})) \\ &= \sum_{i=1}^n \mu^*(X \cap A_i) + \mu^*(X \cap A_{n+1}) \\ &= \sum_{i=1}^{n+1} \mu^*(X \cap A_i) \end{aligned}$$

⊢

We can relax the condition on a set being a member of \mathcal{C}_μ if we know that the domain \mathcal{C} from which we started is an algebra, and that μ is additive on \mathcal{C} . Then we do not have to test whether a μ -measurable set splits all the subsets of S , but it is rather sufficient that A splits X , to be specific:

Proposition 1.127 *Let \mathcal{C} be an algebra, and $\mu : \mathcal{C} \rightarrow [0, +\infty]$ be additive. Then $A \in \mathcal{C}_\mu$ iff $\mu^*(A) + \mu^*(X \setminus A) = \mu^*(X)$.*

Proof This is a somewhat lengthy and laborious computation similarly to the one above, see [Bog07, 1.11.7, 1.11.8]. ⊢

Returning to the general discussion, we have:

Proposition 1.128 *\mathcal{C}_μ is a σ -algebra, and μ^* is countably additive on \mathcal{C}_μ .*

Proof 0. Let $(A_n)_{n \in \mathbb{N}}$ be a countable family of mutually disjoint sets in \mathcal{C}_μ , then we have to show that $A := \bigcup_{n \in \mathbb{N}} A_n \in \mathcal{C}_\mu$, thus we have to show that

$$\mu^*(X \cap A) + \mu^*(X \cap A^c) \leq \mu^*(X)$$

for each $X \subseteq S$ (here \cdot^c is complementation again). Fix X .

1. We know that \mathcal{C}_μ is closed under finite unions, so we have for each $n \in \mathbb{N}$

$$\begin{aligned} \mu^*(X) &\geq \sum_{i=1}^n \mu^*(X \cap A_i) + \mu^*(X \cap \bigcap_{i=1}^n A_i^c) \\ &\geq \sum_{i=1}^n \mu^*(X \cap A_i) + \mu^*(X \cap A), \end{aligned}$$

because $\bigcap_{i=1}^n A_i^c \supseteq A^c$. Letting $n \rightarrow \infty$ we obtain the desired inequality.

3. Thus \mathcal{C}_μ is closed under disjoint countable unions. Using the first entrance trick (Exercise 35) and the observation that \mathcal{C}_μ is an algebra by Proposition 1.125, we convert each countable union into a disjoint countable union, so we have shown that \mathcal{C}_μ is a σ -algebra. Countable additivity of μ^* on \mathcal{C}_μ follows from Lemma 1.126 when putting $X := S$. \dashv

Summarizing, we have demonstrated this Extension Theorem.

Theorem 1.129 *Let \mathcal{C} be an algebra over a set S and $\mu : \mathcal{C} \rightarrow [0, \infty]$ monotone and countably additive.*

1. *There exists an extension of μ to a measure on the σ -algebra $\sigma(\mathcal{C})$ generated by \mathcal{C} .*
2. *If μ is σ -finite, i.e., if S can be written as $S = \bigcup_{n \in \mathbb{N}} S_n$ with $S_n \in \mathcal{C}$ and $\mu(S_n) < \infty$ for all $n \in \mathbb{N}$, then the extension is uniquely determined.*

Proof 1. Proposition 1.128 shows that \mathcal{C}_μ is a σ -algebra containing \mathcal{C} , and that μ^* is a measure on \mathcal{C}_μ . Hence $\sigma(\mathcal{C}) \subseteq \mathcal{C}_\mu$, and we can restrict μ^* to $\sigma(\mathcal{C})$. Denote this restriction also by μ , then μ is a measure on $\sigma(\mathcal{C})$.

2. In order to establish uniqueness, assume first that $\mu(S) < \infty$. Let ν be a measure which extends μ to $\sigma(\mathcal{C})$. Recall the construction of $\sigma(\mathcal{C})$ through transfinite induction on page 47. We claim that

$$\mu(A) = \nu(A) \text{ for all } A \in \mathcal{C}_\zeta$$

holds for all ordinals $\zeta < \omega$. Because \mathcal{C} is an algebra, it is easy to see that for odd ordinals ζ a set $A \in (\mathcal{C}_\zeta)_\delta$ iff there exists a decreasing sequence $(A_n)_{n \in \mathbb{N}} \subseteq \mathcal{C}_\zeta$ with $A = \bigcap_{n \in \mathbb{N}} A_n$; similarly, each element of $(\mathcal{C}_\zeta)_\sigma$ can be represented as the union of an increasing sequence of elements of \mathcal{C}_ζ if ζ is even. Assume for the induction step that ζ is odd, and let $A \in \mathcal{C}_{\zeta+1}$, thus $A = \bigcap_{n \in \mathbb{N}} A_n$ with $A_1 \supseteq A_2 \supseteq \dots$ and $A_n \in \mathcal{C}_\zeta$. Hence by Lemma 1.120

$$\mu(A) = \mu\left(\bigcap_{n \in \mathbb{N}} A_n\right) = \inf_{n \in \mathbb{N}} \mu(A_n) = \inf_{n \in \mathbb{N}} \nu(A_n) = \nu(A).$$

Thus μ and ν coincide on $\mathcal{C}_{\zeta+1}$, if ζ is odd. One argues similarly, but with a monotone increasing sequence in the case that ζ is even. If μ and ν coincide on all \mathcal{C}_η for all η with $\eta < \zeta$ for a limit number ζ , then it is clear that they also coincide on \mathcal{C}_ζ as well.

3. Assume that $\mu(S) = \infty$, but that there exists a sequence $(S_n)_{n \in \mathbb{N}}$ in \mathcal{C} with $\mu(S_n) < \infty$. Because $\mu(S_1 \cup \dots \cup S_n) \leq \mu(S_1) + \dots + \mu(S_n) < \infty$, we may and do assume that the sequence is monotonically increasing. Let $\mu_n(A) := \mu(A \cap S_n)$ be the localization of μ to S_n . μ_n has a unique extension to $\sigma(\mathcal{C})$, and since we have $\mu(A) = \sum_{n \in \mathbb{N}} \mu_n(A)$ for all $A \in \sigma(\mathcal{C})$, the assertion follows. \dashv

But we are not quite done yet, witnessed by a glance at Lebesgue measure. There we started from the semiring of intervals, but our uniqueness theorem states only what happens when we carry out our extension process starting from an algebra. It turns out to be most convenient to have a closer look at the construction of σ -algebras when the family of sets we start from has already some structure. This gives the occasion to introduce Dynkin's π - λ -Theorem. This is an important tool, which makes it sometimes simpler to identify the σ -algebra generated from some family of sets.

Theorem 1.130 (π - λ -Theorem) *Let \mathcal{P} be a family of subsets of S that is closed under finite intersections (this is called a π -class). Then $\sigma(\mathcal{P})$ is the smallest λ -class containing \mathcal{P} ,*

where a family \mathcal{L} of subsets of S is called a λ -class iff it is closed under complements and countable disjoint unions.

Proof 1. Let \mathcal{L} be the smallest λ -class containing \mathcal{P} , then we show that \mathcal{L} is a σ -algebra.

2. We show first that it is an algebra. Being a λ -class, \mathcal{L} is closed under complementation. Let $A \subseteq S$, then $\mathcal{L}_A := \{B \subseteq S \mid A \cap B \in \mathcal{L}\}$ is a λ -class again: if $A \cap B \in \mathcal{L}$, then

$$A \cap (S \setminus B) = A \setminus B = S \setminus ((A \cap B) \cup (S \setminus A)),$$

which is in \mathcal{L} , since $(A \cap B) \cap S \setminus A = \emptyset$, and since \mathcal{L} is closed under disjoint unions.

If $A \in \mathcal{P}$, then $\mathcal{P} \subseteq \mathcal{L}_A$, because \mathcal{P} is closed under intersections. Because \mathcal{L}_A is a λ -system, this implies $\mathcal{L} \subseteq \mathcal{L}_A$ for all $A \in \mathcal{P}$. Now take $B \in \mathcal{L}$, then the preceding argument shows that $\mathcal{P} \subseteq \mathcal{L}_B$, and again we may conclude that $\mathcal{L} \subseteq \mathcal{L}_B$. Thus we have shown that $A \cap B \in \mathcal{L}$, provided $A, B \in \mathcal{L}$, so that \mathcal{L} is closed under finite intersections. Thus \mathcal{L} is a Boolean algebra.

3. \mathcal{L} is a σ -algebra as well. It is enough to show that \mathcal{L} is closed under countable unions. But since

$$\bigcup_{n \in \mathbb{N}} A_n = \bigcup_{n \in \mathbb{N}} \left(A_n \setminus \bigcup_{i=1}^{n-1} A_i \right),$$

this follows immediately. \dashv

Consider an immediate and fairly typical application. It states that two finite measures are equal on a σ -algebra, provided they are equal on a generator which is closed under finite intersections. The proof technique is worth noting: We collect all sets for which the assertion holds into one family of sets and investigate its properties, starting from an originally given set. If we find that the family has the desired property, then we look at the corresponding closure. To be specific, have a look at the proof of the following statement.

Lemma 1.131 *Let μ, ν be finite measures on a σ -algebra $\sigma(\mathcal{B})$, where \mathcal{B} is a family of sets which is closed under finite intersections. Then $\mu(A) = \nu(A)$ for all $A \in \sigma(\mathcal{B})$, provided $\mu(B) = \nu(B)$ for all $B \in \mathcal{B}$.*

Proof We have a look at all sets for which the assertion is true, and investigate this set. Put

$$\mathcal{G} := \{A \in \sigma(\mathcal{B}) \mid \mu(A) = \nu(A)\},$$

then \mathcal{G} has these properties:

- $\mathcal{B} \subseteq \mathcal{G}$ by assumption.
- Since \mathcal{B} is closed under finite intersections, $S \in \mathcal{B} \subseteq \mathcal{G}$.
- \mathcal{G} is closed under complements.
- \mathcal{G} is closed under countable disjoint unions; in fact, let $(A_n)_{n \in \mathbb{N}}$ be a sequence of mutually disjoint sets in \mathcal{G} and $A := \bigcup_{n \in \mathbb{N}} A_n$, then

$$\mu(A) = \sum_{n \in \mathbb{N}} \mu(A_n) = \sum_{n \in \mathbb{N}} \nu(A_n) = \nu(A),$$

hence $A \in \mathcal{G}$.

But this means that \mathcal{G} is a λ -class containing \mathcal{B} . But the smallest λ -class containing \mathcal{G} is $\sigma(\mathcal{B})$ by Theorem 1.130, so that we have now

$$\sigma(\mathcal{B}) \subseteq \mathcal{G} \subseteq \sigma(\mathcal{B}),$$

the last inclusion coming from the definition of \mathcal{G} . Thus we may conclude that $\mathcal{G} = \sigma(\mathcal{B})$, hence all sets in $\sigma(\mathcal{B})$ have the desired property. \dashv

We obtain as a slight extension to Theorem 1.129

Theorem 1.132 *Let \mathcal{C} be a semiring over a set S and $\mu : \mathcal{C} \rightarrow [0, \infty]$ monotone and countably additive.*

1. *There exists an extension of μ to a measure on the σ -algebra $\sigma(\mathcal{C})$ generated by \mathcal{C} .*
2. *If μ is σ -finite, then the extension is uniquely determined.*

\dashv

The assumption on μ being σ -finite is in fact necessary:

Example 1.133 Let \mathcal{S} be the semiring of all left open, right closed intervals on \mathbb{R} , and put

$$\mu(I) := \begin{cases} 0 & \text{if } I = \emptyset, \\ \infty, & \text{otherwise.} \end{cases}$$

Then μ has more than one extension to $\sigma(\mathcal{S})$. For example, let $c > 0$ and put $\nu_c(A) := c \cdot |A|$ with $|A|$ as the number of elements of A . Plainly, ν_c extends μ for every c . \mathfrak{F}

Consequently, the assumption that μ is σ -finite cannot be omitted in order to make sure that the extension is uniquely determined.

1.6.4 μ -Measurable Sets

But Carathéodory's approach gives even more than an extension to the σ -algebra generated from a semiring. This is what we will discuss next in order to find a connection with the discussion about the Axiom of Choice.

Fix for the time being an outer measure μ on $\mathcal{P}(S)$ which we assume as finite. Call $A \subseteq S$ a μ -null set iff we can find a μ -measurable set A_1 with $A \subseteq A_1$ and $\mu(A_1) = 0$. Thus a μ -null set is covered by a measurable set which has μ -measure 0. Because $\mu(X \cap S \setminus A) \leq \mu(X)$ for every $X \subseteq S$, and because an outer measure is monotone, we conclude that each μ -null set is itself μ -measurable. In the same way we conclude that each set A which can be squeezed between two μ -measurable sets of the same measure (hence $A_1 \subseteq A \subseteq A_2$ with $\mu(A_1) = \mu(A_2)$) must be μ -measurable, because in this case $A \setminus A_1 \subseteq A \setminus A_2$ with $\mu(A \setminus A_2) = 0$. Hence \mathcal{C}_μ is *complete* in the sense that any A which can be sandwiched in this way is a member of \mathcal{C}_μ .

This is a characterization of \mathcal{C}_μ using these ideas.

Corollary 1.134 *Let \mathcal{C} be an algebra over a set S and $\mu : \mathcal{C} \rightarrow \mathbb{R}_+$ monotone and countably additive with $\mu(\emptyset) = 0$. Then these statements are equivalent for $A \subseteq S$:*

1. $A \in \mathcal{C}_\mu$.
2. There exists $A_1, A_2 \in \sigma(\mathcal{C})$ with $A_1 \subseteq A \subseteq A_2$ and $\mu(A_1) = \mu(A_2)$.

Proof The implication $2 \Rightarrow 1$ follows from the discussion above, so we will look at $1 \Rightarrow 2$. But this is trivial. \dashv

Having a look at this development, we see that we can extend our measure far beyond the σ -algebra which is generated from the given semiring. One might suspect even that this extension process gives us the whole power set of the set we started from as the domain for the extended measure. That would of course be tremendously practical because we then could assign a measure to each subset. But, alas, if the Axiom of Choice is assumed, these hopes are shattered. The following example demonstrates this. Before discussing it, however, we define and characterize μ -measurable sets on a σ -algebra.

If μ is a finite measure on σ -algebra \mathcal{B} , we can define the outer measure $\mu^*(A)$ for any subset $A \subseteq S$ as we did for functions on a semiring. But since the algebraic structure of a σ -algebra is richer, it is not difficult to see that

$$\mu^*(A) = \inf\{\mu(B) \mid B \in \mathcal{B}, A \subseteq B\}.$$

This is so because a cover of the set A through a countable union of elements on \mathcal{B} is the same as the cover of A through an element of \mathcal{B} , because the σ -algebra \mathcal{B} is closed under countable unions. In a similar way we can try to approximate A from the inside, defining the *inner measure* through

$$\mu_*(A) := \sup\{\mu(B) \mid B \in \mathcal{B}, A \supseteq B\}.$$

So $\mu_*(A)$ is the best approximation from the inside that is available to us. Of course, if $A \in \mathcal{B}$ we have $\mu^*(A) = \mu(A) = \mu_*(A)$, because apparently A is the best approximation to itself.

We can perform the approximation through a sequence of sets, so we are able to precisely fix the inner and the outer measure through elements of the σ -algebra.

Lemma 1.135 *Let $A \subseteq S$ and μ be a finite measure on the σ -algebra \mathcal{B} .*

1. *There exists $A^* \in \mathcal{B}$ such that $\mu^*(A) = \mu(A^*)$.*
2. *There exists $A_* \in \mathcal{B}$ such that $\mu_*(A) = \mu(A_*)$.*

Proof We demonstrate only the first part. For each $n \in \mathbb{N}$ there exists $A_n \in \mathcal{B}$ such that $A \subseteq B_n$ and $\mu(B_n) < \mu(A) + 1/n$. Put $A_n := B_1 \cap \dots \cap B_n \in \mathcal{B}$, then $A \subseteq A_n$, $\mu(A_n) < \mu(A) + 1/n$, and $(A_n)_{n \in \mathbb{N}}$ decreases. Let $A^* := \bigcap_{n \in \mathbb{N}} A_n \in \mathcal{B}$, then $\mu(A^*) = \inf_{n \in \mathbb{N}} \mu(A_n) = \mu^*(A)$ by the second part of Lemma 1.120, because $\mu(A_1) < \infty$. \dashv

The set A^* could be called the measurable closure of A , similarly, A_* its measurable kernel. Using this terminology, we call a set μ -measurable iff its closure and its kernel give the same value.

Definition 1.136 *Let μ be a finite measure on the σ -algebra \mathcal{B} . $A \subseteq S$ is called μ -measurable iff $\mu_*(A) = \mu^*(A)$.*

Every set in \mathcal{B} is μ -measurable, and \mathcal{B}_μ is the σ -algebra of all μ -measurable sets.

The example which has been announced above shows us that under the assumption of (AC) not every subset of the unit interval is λ -measurable, where λ is Lebesgue measure. Hence we will present a set the inner and the outer measure of which are different.

Example 1.137 Define $x \alpha y$ iff $x - y$ is rational for $x, y \in [0, 1]$. Then α is an equivalence relation, because the sum of two rational numbers is a rational number again. This is sometimes called *Vitali's equivalence relation*. The relation α partitions the interval $[0, 1]$ into equivalence classes. Select from each equivalence class an element (which we can do by (AC)), denote the set of selected elements by V . Hence $V \cap [x]_\alpha$ contains for each $x \in [0, 1]$ exactly one element. We want to show that V is not λ -measurable, where λ is Lebesgue measure.

The set $P := \mathbb{Q} \cap [0, 1]$ is countable. Define $V_p := \{v + p \mid v \in V\}$, for $p \in P$. If $p, q \in P$ are different, $V_p \cap V_q = \emptyset$, since $v_1 + p = v_2 + q$ implies $v_1 - v_2 = q - p \in \mathbb{Q}$, thus $v_1 \alpha v_2$, so v_1 and v_2 are in the same class, hence $v_1 = v_2$, thus $p = q$, which is a contradiction.

Put $A := \bigcup_{p \in P} V_p$, then $[0, 1] \subseteq A \subseteq [0, 2]$: Take $x \in [0, 1]$, then there exists $v \in V$ with $x \alpha v$, thus $r := x - v \in \mathbb{Q}$, hence $x \in V_r$. On the other hand, if $x \in V_r$, then $x = v + r$, hence $0 \leq x \leq 2$.

If A is λ -measurable, then $\lambda(A) = 0$ is impossible, because this would imply $\lambda([0, 1]) = 0$, since λ is monotone. Thus $\lambda(A) > 0$. But $\lambda(V_p) = \lambda(V)$ for each p , so that $\lambda(A) = \infty$ by countable additivity. But this contradicts $\lambda([0, 2]) = 2$. Hence A is not λ -measurable, which implies that V is not λ -measurable. \mathfrak{M}

1.7 Games

We have two players, *Angel* and *Demon*, playing against each other. For simplicity, we assume that *playing* means offering a natural number, and that the game — like True Love — never ends. Let A be a set of infinite sequences of natural numbers, then the game G_A is played as follows. Angel starts with $a_0 \in \mathbb{N}$, Demon answers with $b_0 \in \mathbb{N}$, taking Angel's move a_0 into account. Angel replies with a_1 , taking the game's history $\langle a_0, b_0 \rangle$ into account, then Demon answers with b_1 , contingent upon $\langle a_0, b_0, a_1 \rangle$, and so on. Angel wins this game, if the sequence $\langle a_0, b_0, a_1, b_1, \dots \rangle$ is a member of A , otherwise Demon wins.

Let us have a look at strategies. Define

$$\mathcal{N} := \mathbb{N}^{\mathbb{N}}$$

as the set of all sequences of natural numbers, and let

$$\mathcal{S} := \bigcup \{ \langle n_1, \dots, n_k \rangle \mid k \geq 0, n_1, \dots, n_k \in \mathbb{N} \}$$

be the set of all finite sequences of natural numbers (with ϵ as the empty sequence). For easier notation later on, we define appending an element to a finite sequence by $\langle n_1, \dots, n_k \rangle \frown n := \langle n_1, \dots, n_k, n \rangle$. \mathcal{S}_u and \mathcal{S}_g denote all sequences of odd, resp., even, length, the empty sequence is denoted by ϵ , we assume $\epsilon \in \mathcal{S}_g$.

A *strategy* σ for Angel is a map $\sigma : \mathcal{S}_g \rightarrow \mathbb{N}$ which works in the following way: $a_0 := \sigma(\epsilon)$ is the first move of Angel, Demon replies with b_0 , then Angel answers with $a_1 := \sigma(a_0, b_0)$, Demon reacts with b_1 , which Angel answers with $a_2 := \sigma(a_0, b_0, a_1, b_1)$, and so on. If Angel

plays according to strategy σ and Demon's moves are given by $b := \langle b_0, b_1, \dots \rangle \in \mathcal{N}$, then the game's events are collected in $\sigma * b \in \mathcal{N}$; hence $\sigma * b = \langle a_0, b_0, a_1, b_1, \dots \rangle$ with $a_{2k+1} = \sigma(a_0, b_0, \dots, a_{2k}, b_{2k})$ for $k \geq 0$ and $a_0 = \sigma(\epsilon)$. Similarly, a strategy τ for Demon is a map $\tau : \mathcal{S}_u \rightarrow \mathbb{N}$, working in this manner: If Angel plays a_0 , Demon answers with $b_0 := \tau(a_0)$, then Angel plays a_1 , to which Demon replies with $b_1 := \tau(a_0, b_1, a_1)$, and so on. If Angel's moves are collected in $a := \langle a_0, a_1, \dots \rangle$, and if Demon plays strategy τ , then the entire game is recorded in the sequence $a * \tau$. Thus $a * \tau = \langle a_0, b_0, a_1, b_1, \dots \rangle$ with $b_k = \tau(a_0, b_0, \dots, a_k)$ for $k \geq 0$.

Definition 1.138 $\sigma : \mathcal{S}_g \rightarrow \mathbb{N}$ is a winning strategy for Angel in game G_A iff

$$\{\sigma * b \mid b \in \mathcal{N}\} \subseteq A,$$

$\tau : \mathcal{S}_u \rightarrow \mathbb{N}$ is a winning strategy for Demon in game G_A iff

$$\{a * \tau \mid a \in \mathcal{N}\} \subseteq \mathcal{N} \setminus A.$$

It is clear that at most one of Angel and Demon can have a winning strategy. Suppose that in the contrary both have one, say, σ for Angel and τ for Demon. Then $\sigma * \tau \in A$, since σ is winning for Angel, and $\sigma * \tau \notin A$, since τ is winning for Demon. So this assumption does not make sense.


We have a look at *Banach-Mazur games*, another formulation of games which is sometimes more convenient. Each Banach-Mazur game can be transformed into a game which we have defined above.

Before discussing it, it will be convenient to introduce some notation. Let $a, b \in \mathcal{S}$, hence a and b are finite sequences of natural numbers. We say that $a \preceq b$ iff a is an *initial piece* of b (including $a = b$), so there exists $c \in \mathcal{S}$ with $b = ac$; c is denoted by b/a . If we want to exclude equality, we write $a \prec b$.

Example 1.139 The game is played over \mathcal{S} , a subset $B \subseteq \mathcal{N}$ indicates a winning situation. Angel plays $a_0 \in \mathcal{S}$, Demon plays b_0 with $a_0 \preceq b_0$, then Angel plays a_1 with $a_0 b_0 \preceq a_1$, etc. Angel wins this game iff the finite sequence $a_0 b_0 a_1 b_1 \dots$ converges to an infinite sequence $x \in B$.

We encode this game in the following way. \mathcal{S} is countable by Proposition 1.5, so write this set as $\mathcal{S} = \{r_n \mid n \in \mathbb{N}\}$. Put

$$A := \{\langle w_0, w_1, \dots \rangle \mid r_{w_0} \preceq r_{w_1} \preceq r_{w_2} \dots \text{ converges to a sequence in } B\}.$$

It is then immediate that Angel has a strategy for winning the Banach-Mazur game iff it has one for winning that game G_A . 

1.7.1 Determined Games

Games in which neither Angel nor Demon have a winning strategy are somewhat, well, indeterminate and might be avoided. We see some similarity between a strategy and the selection argument in $(\mathbb{A}C)$, because a strategy selects an answer among several possible choices, while a choice function picks elements, each from a given set. This intuitive similarity will be investigated now.

Definition 1.140 A game G_A is called *determined* iff either Angel or Demon has a winning strategy.

Suppose that each game G_A is determined, no matter what set $A \subseteq \mathcal{N}$ we chose, then we can define a choice function for countable families of non-empty subsets of \mathcal{N} .

Theorem 1.141 Assume that each game is determined. Then there exists a choice function for countable families of non-empty subsets of \mathcal{N} .

Proof 1. Let $\mathcal{F} := \{X_n \mid n \in \mathbb{N}\}$ be a countable family with $\emptyset \neq X_n \subseteq \mathcal{N}$ for $n \in \mathbb{N}$. We will define a function $f : \mathcal{F} \rightarrow \mathcal{N}$ such that $f(X_n) \in X_n$ for all $n \in \mathbb{N}$. The idea is to play a game which Angel cannot win, hence for which Demon has a winning strategy. To be specific, if Angel plays $\langle a_0, a_1, \dots \rangle$ and Demon plays $b := \langle b_0, b_1, \dots \rangle$, then Demon wins iff $b \in X_{a_0}$. Since by assumption Demon has a winning strategy τ , we then put

$$f(X_n) := \langle n, 0, 0, \dots \rangle * \tau.$$

2. Let us look at this idea. Put

$$A := \{\langle x_0, x_1, \dots \rangle \in \mathcal{N} \mid \langle x_1, \dots \rangle \notin X_{x_0}\}.$$

Suppose that Angel starts upon playing a_0 . Since $X_{a_0} \neq \emptyset$, Demon can take an arbitrary $b \in X_{a_0}$ and plays $\langle b_0, b_1, \dots \rangle$. Hence Angel cannot win, so B has a winning strategy τ .

3. Now look at $\langle n, 0, 0, \dots \rangle * \tau \notin A$, because τ is a winning strategy. From the definition of A we see that this is an element of X_n , so we have found a choice function indeed. \dashv

The space \mathcal{N} looks a bit artificial, just as a mathematical object to play around with. But this is not the case. It can be shown that there exists a bijection $\mathcal{N} \rightarrow \mathbb{R}$ with some desirable properties (we will not enter into this construction, however). With this in mind, we state as a consequence

Corollary 1.142 Assume that each game is determined. Then there exists a choice function for countable families of non-empty subsets of \mathbb{R} . \dashv

Let us fix the existence of a winning strategy for either Angel or Demon in an axiom, the *Axiom of Determinacy*.

(\mathbb{AD}) Each game is determined.

Given Corollary 1.142, the relationship of the Axiom of Determinacy to the Axiom of Choice is of interest. Does (\mathbb{AD}) imply (\mathbb{AC}) ? The hope of establishing this are shattered, however, by this observation.

Proposition 1.143 If (\mathbb{AC}) holds, there exists $A \subseteq \mathcal{N}$ such that G_A is not determined.

Before entering the proof, we observe that the set of all strategies S_A for Angel resp. S_D for Demon has the same cardinality as the power set $\mathcal{P}(\mathbb{N})$ of \mathbb{N} .

Proof 0. We have to find a set $A \subseteq \mathcal{N}$ such that neither Angel nor Demon has a winning strategy for the game G_A . By (\mathbb{AC}) , the sets S_A resp. S_D can be well-ordered, by the

observation just made we can write

$$\begin{aligned} S_A &= \{\sigma_\alpha \mid \alpha < \omega\}, \\ S_D &= \{\tau_\alpha \mid \alpha < \omega\}. \end{aligned}$$

1. We will construct now disjoint sets $X = \{x_\alpha \mid \alpha < \omega\} \subseteq \mathcal{N}$ and $Y = \{y_\alpha \mid \alpha < \omega\} \subseteq \mathcal{N}$ indexed by $\{\alpha \mid \alpha < \omega\}$, which will help define the game. Suppose x_β and y_β are defined for all $\beta < \alpha$. Then, because α is countable, the sets $\{x_\beta \mid \beta < \alpha\}$ and $\{y_\beta \mid \beta < \alpha\}$ are countable as well, and there are uncountably many $b \in \mathcal{N}$ such that $\sigma_\alpha * b \notin \{x_\beta \mid \beta < \alpha\}$. Take one of them and put $y_\alpha := \sigma_\alpha * b$. For the same reason, there are uncountably many $a \in \mathcal{N}$ such that $a * \tau_\alpha \notin \{y_\beta \mid \beta \leq \alpha\}$; take one of them and put $x_\alpha := a * \tau_\alpha$.
2. Clearly, X and Y are disjoint. Angel does not have a strategy for winning game G_X . Suppose it has a winning strategy σ , so that $\sigma = \sigma_\alpha$ for some $\alpha < \omega$. But $y_\alpha = \sigma_\alpha * b \notin X$ by construction, which is a contradiction. One similarly shows that Demon cannot have a winning strategy for game G_X . Hence this game is not determined. \dashv

1.7.2 Proofs Through Games

We will show now that games are a tool for proofs. The basic idea is to attach a statement to a game, and if Angels has a strategy for winning the game, then the statement is established, otherwise it is not. Hence we have to encode the statement in such a way that this mechanism can be used, but we have also to establish a scenario in which to argue. The formulation chosen suggests that Angel has to have a winning strategy for winning a game, which in turn suggests that we assume a framework in which games are determined. But we have seen above that this is not without conflicts when considering (AC). This section is devoted to establish that every subset of the unit interval is Lebesgue measurable, provided each game is determined. We have seen in Example 1.137 that (AC) implies that there exists a set which is not Lebesgue measurable. Hence “it is natural to postulate that Determinacy holds to the extent that it does not contradict the Axiom of Choice”, as T. Jech writes in his massive treatise of Set Theory [Jec06, p. 628].

The Goal. We want to show that each subset of the unit interval is measurable, provided each game is determined. This is based on the observation that it is sufficient to establish that $\lambda_*(A) > 0$ or $\lambda_*([0, 1] \setminus A) > 0$ for each and every subset $A \subseteq [0, 1]$, where, as above, λ is Lebesgue measure on the unit interval. This is the reason:

Lemma 1.144 *Assume that there exists a subset of the unit interval which is not λ -measurable. Then there exists a subset $M \subseteq [0, 1]$ with $\lambda_*(M) = 0$ and $\lambda^*(M) = 1$. \dashv*

The Basic Approach. Given an arbitrary subset $X \subseteq [0, 1]$, we will define a game G_X such that if there exists a winning strategy for Angel, then we can find a measurable subset $A \subseteq X$ which has positive Lebesgue measure (hence $\lambda_*(X) > 0$). If there exists, however, a winning strategy for Demon, then we can find a measurable subset $A \subseteq [0, 1]$ with positive Lebesgue measure such that $A \cap X = \emptyset$ (hence $\lambda_*([0, 1] \setminus A) > 0$).

Little Helpers. We need some preparations before we start. So let's get on with it now as not to interrupt the flow of discussion later on.

Lemma 1.145 *Let $(F_n)_{n \in \mathbb{N}}$ be a sequence of non-empty subsets of the unit interval $[0, 1]$ such that*

1. *Each F_n is a finite union of closed intervals.*
2. *The sequence is monotonically decreasing, hence $F_1 \supseteq F_2 \supseteq \dots$*
3. *The sequence of diameters $\text{diam}(F_n) := \sup_{x, y \in F_n} |x - y|$ tends to zero.*

Then there exists a unique $p \in [0, 1]$ with $\{p\} = \bigcap_{n \in \mathbb{N}} F_n$.

Proof 1. It is clear from the last condition that there can be at most one point in the intersection of this sequence. Suppose there are two distinct points p, q in this intersection, then $\delta := |p - q| > 0$. But there exists some $n_0 \in \mathbb{N}$ with $\text{diam}(F_m) < \delta$ for all $m \geq n_0$. This is a contradiction.

2. Assume that $\bigcap_{n \in \mathbb{N}} F_n = \emptyset$. Put $G_n := [0, 1] \setminus F_n$, then G_n is the union of a finite number of open intervals, say $G_n = H_{n,1} \cup \dots \cup H_{n,k_n}$, and $[0, 1] \subseteq \bigcup_{n \in \mathbb{N}} G_n$. By the Heine-Borel Theorem 1.88 there exist a finite set of intervals H_{n_i, j_i} with $1 \leq i \leq r, 1 \leq j_i \leq k_{n_i}$ such that $[0, 1] \subseteq \bigcup_{i=1}^r H_{n_i, j_i}$. Because the sequence of the F_n decreases, the sequence $(G_n)_{n \in \mathbb{N}}$ is increasing, so we find an index N such that $H_{n_i, j_i} \subseteq G_N$ for $1 \leq i \leq r, 1 \leq j_i \leq k_{n_i}$. But this means $[0, 1] \subseteq G_N$, thus $F_N = \emptyset$, contradicting the assumption that all F_n are non-empty. \dashv

Another preparation concerns the convergence of an infinite product.

Lemma 1.146 *Let $(a_n)_{n \in \mathbb{N}}$ be a sequence of real numbers with $0 < a_n < 1$ for all $n \in \mathbb{N}$. Then the following statements are equivalent*

1. $\prod_{i \in \mathbb{N}} (1 - a_i) := \lim_{n \rightarrow \infty} \prod_{i=1}^n (1 - a_i)$ exists.
2. $\sum_{n \in \mathbb{N}} a_n$ converges.

Proof One shows easily by induction on n that

$$\prod_{i=1}^n (1 - a_i) > 1 - \left(\sum_{i=1}^n a_i \right)$$

for $n \geq 2$. Since $0 < a_n < 1$ for all $n \in \mathbb{N}$, this implies the equivalence. \dashv

This has an interesting consequence, viz., that we have a positive infinite product, provided the corresponding series converges. To be specific:

Corollary 1.147 *Let $(a_n)_{n \in \mathbb{N}}$ be a sequence of real numbers with $0 < a_n < 1$ for all $n \in \mathbb{N}$. Then the following statements are equivalent*

1. $\prod_{i \in \mathbb{N}} (1 - a_i)$ is positive.
2. $\sum_{n \in \mathbb{N}} a_n$ converges.

Proof 1. Put $Q_k := \prod_{i=1}^k a_i$, $Q := \lim_{k \rightarrow \infty} Q_k$. Assume that $\sum_{n \in \mathbb{N}} a_n$ converges, then there exists $m \in \mathbb{N}$ such that $\sigma_m := \sum_{i=m}^{\infty} a_i < 1$. Hence we have

$$\frac{Q_n}{Q_m} > 1 - (a_{m+1} + \dots + a_n) > 1 - \sigma_m$$

for $n > m$, so that

$$Q = \lim_{k \rightarrow \infty} Q_k > Q_m \cdot (1 - \sigma_m) > 0.$$

2. On the other hand, if the series diverges, then we can find an index m for $N \in \mathbb{N}$ such that $a_1 + \dots + a_n > N$ whenever $n > m$. Hence

$$\prod_{n \in \mathbb{N}} \frac{1}{1 - a_n} \leq \lim_{k \rightarrow \infty} \frac{1}{1 - (a_1 + \dots + a_k)} = 0$$

+

This observation will be helpful when looking at our game.

The Game. Before discussing the game proper, we set the stage. Fix a sequence $(r_n)_{n \in \mathbb{N}}$ of reals such that $\sum_{n \in \mathbb{N}} r_n < 1$ and $1/2 > r_1 > r_2 > \dots$.

Let $k \in \mathbb{N}$ be a natural number, and define \mathcal{J}_k as the collection of sets S with these properties

- $S \subseteq [0, 1]$ is a finite union of closed intervals with rational end points.
- The *diameter* $\text{diam}(S) = \sup_{x, y \in S} |x - y|$ of S is smaller than $1/2^k$.
- The Lebesgue measure $\lambda(S)$ of S is $r_1 \cdot \dots \cdot r_k$.

Put $\mathcal{J}_0 := \{[0, 1]\}$ as the mandatory first draw of Angel. Note that \mathcal{J}_k is countable for all $k \in \mathbb{N}$, so that $\bigcup_{k \geq 0} \mathcal{J}_k$ is countable as well by Proposition 1.6 (this was proved without using (AC)!).

The game starts. We fix $X \subseteq [0, 1]$ as the Great Prize; this is the set we want to investigate. Angels starts with choosing the unit interval $S_0 := [0, 1]$, Demon chooses a set $S_1 \in \mathcal{J}_1$, then Angel chooses a set $S_2 \in \mathcal{J}_2$ with $S_2 \subset S_1 \subset S_0$, Demon chooses a set $S_3 \subset S_2$ with $S_3 \in \mathcal{J}_3$, and so on. In this way, the game defines a decreasing sequence $(S_n)_{n \in \mathbb{N}}$ of closed sets the diameter of which tends to zero. By Lemma 1.145 there exists exactly one point p with $p \in \bigcap_{n \in \mathbb{N}} S_n$. If $p \in [0, 1] \setminus X$, then Angel wins, if $p \in X$, then Demon wins.

Analysis of the Game. First note that we will not encode the game into a syntactic form according to the definition of G_A . This would require much encoding and decoding between the formal representation and the informal one, so that the basic ideas might get lost. Since life is difficult enough, we stick to the informal representation, trusting that the formal one could easily be derived from it, and focus on the ideas behind the game. After all, we want to prove something through this game which is not entirely trivial.

The game spawns a tree rooted at $S_0 := [0, 1]$ with offsprings all those elements S_1 of \mathcal{J}_1 with $S_1 \subset S_0$. If we are at node $S_k \in \mathcal{J}_k$, then this node has all elements $S \in \mathcal{J}_{k+1}$ as offsprings

for which $S \subset S_k$ holds. Consequently, the tree's depth will be infinite, because the game continues forever. The offsprings of a node will be investigated in a moment.

We define for easier discussion the sets

$$\mathcal{W}_k := \{\langle S_0, \dots, S_k \rangle \in \prod_{i=0}^k \mathcal{J}_i \mid S_0 \supset S_1 \supset \dots \supset S_k\},$$

$$\mathcal{W}^* := \bigcup_{k \geq 0} \mathcal{W}_k$$

as the set of all paths which are possible in this game. Hence Angel chooses initially $S_0 = [0, 1]$, Demon chooses $S_1 \in \mathcal{J}_1$ with $S_1 \subset S_0$ (hence $\langle S_0, S_1 \rangle \in \mathcal{W}_1$), so that $\langle S_0, S_1, S_2 \rangle \in \mathcal{W}_2$, etc. \mathcal{W}_{2n} is the set of all possible paths after the n -th draw of Angel, and \mathcal{W}_{2n+1} yields the state of affairs after the n -th move of Demon.

For an analysis of strategies, we will fix now $k \in \mathbb{N}$ and a map $\Gamma : \mathcal{W}_k \rightarrow \mathcal{J}_{k+1}$ such that $\Gamma(S_0, \dots, S_k) \subset S_k$, hence $\langle S_0, \dots, S_k, \Gamma(S_0, \dots, S_k) \rangle = \langle S_0, \dots, S_k \rangle \frown \Gamma(S_0, \dots, S_k) \in \mathcal{W}_{k+1}$. Just to have a handy name for it, call such a map *admissible at k* .

Lemma 1.148 *Assume Γ is admissible at k . Given $\langle S_0, \dots, S_k \rangle \in \mathcal{W}_k$, there exists $m \in \mathbb{N}$ and a finite sequence $T_{k+1,i} \in \mathcal{J}_{k+1}$ for $1 \leq i \leq m$ such that*

1. $T_{k+1,i} \subset S_k$ for all i ,
2. $\lambda(\bigcup_{i=1}^m \Gamma(S_0, \dots, S_k, T_{k+1,i})) \geq \lambda(S_k) \cdot (1 - 2 \cdot r_{k+1})$,
3. The sets $\Gamma(S_0, \dots, S_k, T_{k+1,1}), \dots, \Gamma(S_0, \dots, S_k, T_{k+1,m})$ are mutually disjoint.

Proof The sets $T_{k+1,i}$ are defined by induction. Assume that $T_{k+1,1}, \dots, T_{k+1,j}$ is already defined for $j \geq 0$, put

$$R_j := S_k \setminus \bigcup_{i=1}^j \Gamma(S_0, S_1, \dots, S_k, T_{k+1,i}).$$

Now we have two possible cases: either

$$(\dagger) \lambda(R_j) > 2 \cdot \lambda(S_k) \cdot r_{k+1}$$

or this inequality is false. Note that $\lambda(S_k) = r_1 \cdot \dots \cdot r_k$, and $1/2 > r_k > r_{k+1}$, so that initially $\lambda(R_0) = \lambda(S_k) > 2 \cdot \lambda(S_k) \cdot r_{k+1}$. Now assume that (\dagger) holds. Because S_k is the union of a finite number of closed intervals, and because R_j does not exhaust S_k , we conclude that R_j contains a subset P with diameter $\text{diam}(P) \leq \text{diam}(R_j) \leq 2^{-(k+1)}$ such that $\lambda(P) > \lambda(S_k)$. We can select P in such a way that it is a finite union of intervals. Then there exists $T_{k+1,j+1} \subseteq P$ which belongs to \mathcal{J}_{k+1} . Take it. Then the first property is satisfied.

This process continues until inequality (\dagger) becomes false, which gives the second property. Because

$$\Gamma(S_0, \dots, S_k, T_{k+1,i}) \subset T_{k+1,i} \subset S_k \setminus \bigcup_{j=1}^{i-1} \Gamma(S_0, \dots, S_k, T_{k+1,j}),$$

we conclude that the sets $\Gamma(S_0, \dots, S_k, T_{k+1,1}), \dots, \Gamma(S_0, \dots, S_k, T_{k+1,m})$ are mutually disjoint. \dashv

Now let τ be a strategy for Demon, hence $\tau : \bigcup_{k \geq 0} \mathcal{W}_{2k+1} \rightarrow \bigcup_{k \leq 0} \mathcal{J}_{2k}$ is a map such that $\tau(S_0, \dots, S_{2k}) \subset S_{2k}$. If the game's history at time k is given by the path $\langle S_0, \dots, S_{2k} \rangle$ with Angels having played S_{2k} as a last move, then the game continues with $\tau(S_0, \dots, S_{2k})$ as Demon's next move, so that the new path is just $\langle S_0, \dots, S_{2k} \rangle \frown \tau(S_0, \dots, S_{2k})$.

Let's see what happens if Angel selects the next move according to Lemma 1.148. Initially, Angels plays S_0 , then Demon plays $\tau(S_0)$, so that the game's history is now $\langle S_0 \rangle \frown \tau(S_0)$; let $T_{0,1}, \dots, T_{0,m_0}$ be the sets selected according to Lemma 1.148 for this history, then the possible continuations in the game are $t_i := \langle S_0 \rangle \frown \tau(S_0) \frown T_{0,i}$ for $1 \leq i \leq m_0$, so that Demon's next move is $t_i \frown \tau(t_i)$, thus

$$K_\tau(\langle S_0 \rangle \frown \tau(S_0)) := \{ \langle S_0 \rangle \frown \tau(S_0) \frown T_{0,i} \frown \tau(\langle S_0 \rangle \frown \tau(S_0) \frown T_{0,i}) \mid 1 \leq i \leq m_0 \} \in \mathcal{W}_3$$

describes all possible moves for Demon in this scenario. Given τ , this depends on S_0 as the history up to that moment, and on the choice to Angel's moves according to Lemma 1.148. To see the pattern, consider Demon's next move. Take $t = \langle t_0, t_1, t_2, t_3 \rangle \in K_\tau(S_0 \frown \tau(S_0))$, then $\tau(t) \in \mathcal{J}_4$ with $\tau(t) \subset t_3$, and choose $T_{1,1}, \dots, T_{1,m_1}$ according to Lemma 1.148 as possible next moves for Angel, so that the set of all possible moves for Demon given this history is an element of the set

$$K_\tau(t) = K_\tau(\langle t_1, t_2, t_3 \rangle \frown \tau(t_1, t_2, t_3)) := \{ t \frown T_{1,i} \frown \tau(t \frown T_{1,i}) \mid 1 \leq i \leq m_1 \} \in \mathcal{W}_5.$$

This provides a window into what is happening. Now let us look at the broader picture. Denote by for $t \in \mathcal{W}_n$ by $J_\tau(t)$ the set $\{ t \frown T_{n,1}, \dots, t \frown T_{n,m} \}$, where $T_{n,1}, \dots, T_{n,m}$ are determined for t and τ according to Lemma 1.148 as the set of all possible moves for Angel. Hence given history t , $J_\tau(t)$ is the set of all possible paths for which Demon has to provide the next move. Then put

$$J_\tau^n := \bigcup_{s_2 \in J_\tau(\langle S_0 \rangle \frown \tau(S_0))} \bigcup_{s_4 \in J_\tau(s_2 \frown \tau(s_2))} \dots \bigcup_{s_{2(n-1)} \in J_\tau(s_{2(n-2)} \frown \tau(s_{2(n-2)}))} J_\tau(s_{2(n-1)} \frown \tau(s_{2(n-1)}))$$

with

$$J_\tau^1 = J_\tau(\langle S_0 \rangle \frown \tau(S_0)).$$

Finally, define

$$A_n := \bigcup \{ \tau(s_{2n}) \mid s_{2n} \in J_\tau^n \}.$$

Hence J_τ^n contains all possible moves of Angel at time $2n$, so that A_n tells us what Demon can do at time $2n + 1$. These are the important properties of $(A_n)_{n \in \mathbb{N}}$:

Lemma 1.149 *We have for all $n \in \mathbb{N}$*

1. $\lambda(A_n) \geq r_1 \cdot \prod_{i=1}^n (1 - 2 \cdot r_{2i})$
2. $A_{n+1} \subset A_n$

Proof 1. The second property follows immediately from Lemma 1.148, so we will focus on the first property. It will be proved by induction on n . We infer from Lemma 1.148 that the sets $\tau(s_{2n})$ are mutually disjoint, when s_{2n} runs through J_τ^n

2. $n = 1$. We obtain immediately from Lemma 1.148 that

$$\begin{aligned}\lambda(A_1) &= \lambda\left(\bigcup\{\tau(s_2) \mid s_2 \in J_\tau(\langle S_0 \rangle \frown \tau(S_0))\}\right) \\ &\geq r_1 \cdot (1 - 2 \cdot r_2)\end{aligned}$$

(set $\Gamma := \tau$ and $k = 1$).

2. Induction step $n \rightarrow n + 1$. We infer from Lemma 1.148 that

$$(\dagger) \lambda\left(\bigcup\{\tau(s_{2(n+1)}) \mid s_{2(n+1)} \in J_\tau(s_{2n})\}\right) \geq \lambda(\tau(s_{2n+1})) \cdot (1 - 2 \cdot r_{2(n+1)}).$$

Disjointness then implies

$$\begin{aligned}\lambda(A_{n+1}) &= \sum_{s_{2n} \in J_\tau^n} \lambda\left(\bigcup\{\tau(s_{2(n+1)}) \mid s_{2(n+1)} \in J_\tau(s_{2n})\}\right) \\ &\geq \sum_{s_{2n} \in J_\tau^n} \lambda(\tau(s_{2n})) \cdot (1 - 2 \cdot r_{2(n+1)}) && \text{(inequality } (\dagger)) \\ &= \lambda\left(\bigcup_{s_{2n} \in J_\tau^n} \tau(s_{2n+1})\right) \cdot (1 - 2 \cdot r_{2(n+1)}) && \text{(disjointness)} \\ &= \lambda(A_n) \cdot (1 - 2 \cdot r_{2(n+1)}) && \text{(induction hypothesis)} \\ &\geq r_1 \cdot \prod_{i=1}^{n+1} (1 - 2 \cdot r_{2i})\end{aligned}$$

⊥

Now we are getting somewhere — we show that we can find for every element in $\bigcap_{n \in \mathbb{N}} A_n$ a strategy so that the moves of Angel and of Demon *converge* to this point. To be more specific:

Lemma 1.150 *Assume that Demon adopts strategy τ . For every point $p \in \bigcap_{n \in \mathbb{N}} A_n$ there exists for Angel a strategy σ_p with this property: If Angel plays σ_p and Demon plays τ , then $\bigcap_{i=0}^\infty S_i = \{p\}$, where S_0, S_1, \dots are the consecutive moves of the players.*

Proof The sets $s_{2n} \in J_\tau^n$ are mutually disjoint for fixed n , so we find a unique sequence $s'_{2n} \in J_\tau^n$ for which $p \in \tau(s'_{2n})$. Represent $s'_{2n} = \langle S_0, \dots, S_{2n} \rangle$, and let σ_p be a strategy for Angel such that $\sigma_p(\langle S_0, \dots, S_{2n-1} \rangle \frown \tau(S_0, \dots, S_{2n-1})) = S_{2n}$ holds. Thus $p \in \bigcap_{n \in \mathbb{N}} S_n$, if Angel plays σ_p and Demon plays τ . ⊥

Now let τ be a winning strategy for Demon, then $A := \bigcap_{n \in \mathbb{N}} A_n \subseteq [0, 1] \setminus X$; this is the outcome if Angel plays one of the strategy in $\{\sigma_p \mid p \in A\}$. There may be other strategies for Angel than the one described above, but no matter how Angel plays the game, we will end up in an element not in X . This implies $\lambda(A) \leq \lambda_*([0, 1] \setminus X)$. But we know from Lemma 1.149 that $\lambda(A) \geq r_1 \cdot \prod_{i=1}^\infty (1 - 2 \cdot r_{2i}) > 0$ by Lemma 1.146 and its corollary, consequently, $\lambda_*([0, 1] \setminus X) > 0$. If, however, Demon does not have a winning strategy, the Angel has one, if we assume that the game is determined. The argumentation is completely the same as above to show that $\lambda_*(X) > 0$.

Thus we have shown:

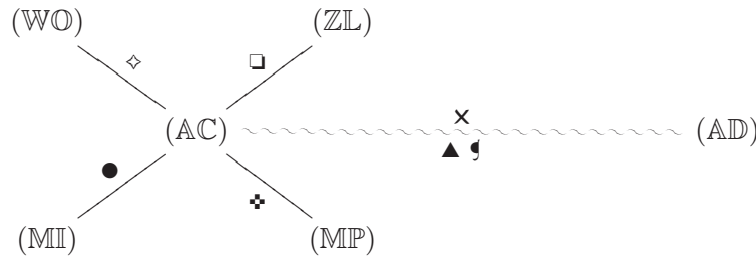
Theorem 1.151 *If each game is determined, then each subset of the unit interval is λ -measurable. \dashv*

We have seen that games are not only just for fun, but are a tool for investigating properties of sets. In fact, one can define games for investigating many topological properties, not all as laborious as the one we have defined above.

1.8 Wrapping it up

This summarizes the discussion. Some hints for further information can be found in the Bibliographic Notes. The Lecture Note [Her06] by H. Herrlich and the list of its references is a particularly rich bag of suggestions for further reading. The discussion in P. Taylor's book [Tay99, p. 58] (“Although we, at the cusp of the century, now reject Choice ...”) is also worth looking at, albeit from a completely different angle.

This is a small diagram indicating the dependencies discussed here.



The symbols provide a directory for the corresponding statements.

◇	Theorem 1.41
□	Proposition 1.42
●	Theorem 1.80
✦	Proposition 1.44
✕	Existence of a non-determined game under (AC), Proposition 1.143
▲	Choice function for countable families under (AD), Theorem 1.141
●	Measurability of every subset of $[0, 1]$ under (AD), Theorem 1.151

1.9 Bibliographic Notes

This chapter contains mostly classical topics. The proof of Cantor's enumeration and its consequences for enumerating the set of all finite sequences of natural numbers is taken from [KM76], so is the discussion of ordinals. Jech's representation [Jec06] has been helpful as well, so was [Gol96]. The books by Davis [Dav00] and by Aczel [Acz00] contain some gripping historical information on the subject of early set theory; the monograph [COP01] discusses implications for computing when the Axiom of Foundations (page 6) is weakened.

Term rewriting is discussed in [BN98]; reduction systems (Example 1.13) are central to it. Aumann's classic [Aum54], unfortunately not as frequently used as this valuable book should

be, helped in discussing Boolean algebras, and the proof for the general distributive law in Boolean algebras as well as some exercises has been taken from [Bir67] and from [DP02], see also [Sta97] for finite lattices. The discussion on measure extension follows quite closely the representation given in the first three chapters of [Bil95] with an occasional glimpse at [Els99] and the awesome [Bog07]. Finally, games are introduced as in [Jec06, Chapter 33], see also [Jec73]; the game-theoretic proofs on measurability are taken from [MS64]. Infinite products are discussed at length in the delightful textbook [Bro08], see also [Chr64]. A general source for this chapter was the exposition by H. Herrlich [Her06], providing a *tour d'horizon*.

1.10 Exercises

Exercise 1 The Axiom of Pairs defines $\langle a, b \rangle := \{\{a\}, \{a, b\}\}$, see page 5. Using the Axioms of ZFC, show that $\langle a, b \rangle = \langle a', b' \rangle$ iff $a = a'$ and $b = b'$.

Exercise 2 Show that $f : A \rightarrow B$ is injective iff $f^{-1} : \mathcal{P}(B) \rightarrow \mathcal{P}(A)$ is surjective; f is surjective iff f^{-1} is injective.

Exercise 3 Define \leq_d on \mathbb{N} as in Example 1.8. Show that p is prime iff p is a minimal element of $\mathbb{N} \setminus \{1\}$.

Exercise 4 Order $S := \mathcal{P}(\mathbb{N}) \setminus \{\mathbb{N}\}$ by inclusion as in Example 4. Show that the set $A := \{2 \cdot n, 2 \cdot n + 1 \mid n \in \mathbb{N}\}$ is bounded in S ; does A have a smallest lower bound?

Exercise 5 Let S be a set, $H : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$ be an order preserving map. Show that $A := \bigcup \{X \in \mathcal{P}(S) \mid X \subseteq H(X)\}$ is a fixed point of H , i.e., satisfies $H(A) = A$. Moreover, A is the greatest fixed point of H , i.e., if $H(Y) = Y$, then $Y \subseteq A$.

Exercise 6 Let $f : X \rightarrow Y$ and $g : Y \rightarrow X$ be maps. Using Exercise 5 show that there exists disjoint subsets X_1 and X_2 of X and disjoint subsets Y_1 and Y_2 of Y such that $X = X_1 \cup X_2$, $Y = Y_1 \cup Y_2$ and $f[X_1] = Y_1$, $g[Y_2] = X_2$. The map $A \mapsto X \setminus g[Y \setminus f[A]]$ might be helpful.

This decomposition is attributed to *S. Banach*.

Exercise 7 Use Exercise 6 for a proof of the Schröder-Bernstein-Theorem 1.2.

Exercise 8 Show that there exist for the bijection J from Proposition 1.3 surjective maps $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ and $L : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ such that $J(K(x), L(x)) = x$, $K(x) \leq x$ and $L(x) \leq x$ for all $x \in \mathbb{N}_0$.

Exercise 9 Construct a bijection from the power set $\mathcal{P}(\mathbb{N})$ to \mathbb{R} using the Schröder-Bernstein-Theorem 1.2.

Exercise 10 Show using the Schröder-Bernstein Theorem 1.2 that the set of all subsets of \mathbb{N} of size exactly 2 is countable. Extend this result by showing that the set of all subsets of \mathbb{N} of size exactly k is countable. Can you show without (AC) that the set of all finite subsets of \mathbb{N} is countable?

Exercise 11 Show that $\omega_1 := \{\alpha \mid \alpha \text{ is a countable ordinal}\}$ is an ordinal (Proposition 1.38). Show that ω_1 is not countable.

Exercise 12 An undirected graph $\mathcal{G} = (V, E)$ has nodes V and (undirected) edges E . An edge connecting nodes x and y be written as $\{x, y\}$; note $x \neq y$. A subgraph $\mathcal{G}' = (G', E')$ of \mathcal{G} is a graph with $G' \subseteq G$ and $E' \subseteq E$. \mathcal{G} is k -colorable iff there exists a map $c : V \rightarrow \{1, \dots, k\}$ such that $c(x) \neq c(y)$, whenever $\{x, y\} \in E$ is an edge in \mathcal{G} . Show that \mathcal{G} is k -colorable iff each of its finite subgraphs is k -colorable.

Exercise 13 Let B be a Boolean algebra, and define $a \oplus b := (a \vee b) \wedge \neg(a \wedge b)$, as in Section 1.5.6. Show that (B, \oplus, \cap) is a commutative ring.

Exercise 14 Complete the proof of Proposition 1.44 by proving that $(\mathbb{AC}) \Rightarrow (\mathbb{MP})$.

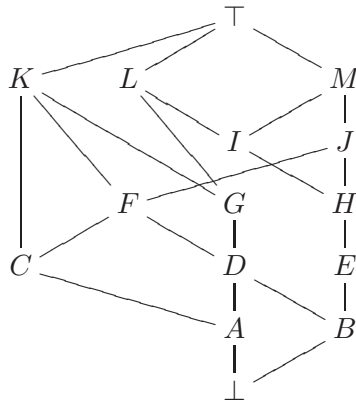
Exercise 15 Complete the proof of Lemma 1.78.

Exercise 16 Using the notation of Section 1.5.1, show that $v^* \models \varphi$ iff $\varphi \in \mathcal{M}^*$ using induction on the structure of φ .

Exercise 17 Do Exercise 12 again, using the Compactness Theorem 1.49.

Exercise 18 Let \mathcal{F} be an ultrafilter over an infinite set S . Show that if \mathcal{F} contains a finite set, then there exists $s \in S$ such that $\mathcal{F} = \mathcal{F}_s$, the ultrafilter defined by s , see Example 1.57.

Exercise 19 Consider this ordered set



Discuss whether these values exist, and determine their values, if they do:

$$\begin{array}{lll}
 D \wedge E; & D \vee E; & (J \wedge L) \wedge K \\
 (L \wedge E) \wedge K; & L \wedge (E \wedge K); & C \wedge E \\
 (C \vee D) \vee E; & \sup\{C, D, E\}; & C \vee (D \vee E) \\
 J \wedge (L \vee K); & (J \wedge L) \vee (J \wedge K); & C \vee G
 \end{array}$$

Exercise 20 Let L be a lattice. An element $s \in L$ with $s \neq \perp$ is called *join irreducible* iff $s = r \vee t$ implies $s = r$ or $s = t$. Element t *covers* element s iff $s < t$, and if $s < v < t$ for no element v . Show that if L is a finite distributive lattice, then s is join irreducible iff s covers exactly one element.

Exercise 21 Let P be a finite partially ordered set. Show that the down set $I \in \mathcal{D}(P)$ is join irreducible iff I is a principal down set.

Exercise 22 Identify the join-irreducible elements in $\mathcal{P}(S)$ for $S \neq \emptyset$ and in the lattice of all open intervals $\{]a, b[\mid a \leq b\}$, both ordered by inclusion.

Exercise 23 Show that in a lattice one distributive law implies the other one.

Exercise 24 Give an example for a down set in a lattice which is not an ideal.

Exercise 25 Show that in a distributive lattice $c \wedge x = c \wedge y$ and $c \vee x = c \vee y$ for some c implies $x = y$.

Exercise 26 Let G be a commutative group, written additively. Show that the subgroups form a lattice under the subset relation.

Exercise 27 Assume that in lattice L there exists for each $a, b \in L$ the relative *pseudo-complement* $b : a$ of a in b ; this is the largest element $x \in L$ such that $a \wedge x \leq b$. Show that a pseudo-complemented lattice is distributive. Furthermore, show that each Boolean algebra is pseudo-complemented. Lattices with pseudo-complements are called *Browerian lattices*.

Exercise 28 A lattice is called *complete* iff it contains suprema and infima for arbitrary subsets. Show that a bounded partially ordered set (L, \leq) is a complete lattice if the infimum

for arbitrary sets exists. Conclude that the set of all equivalence relations on a set form a complete lattice under inclusion.

Exercise 29 Let $S \neq \emptyset$ be a set, $a \in S$. Compute for the Boolean algebra $B := \mathcal{P}(S)$ and the ideal $I := \mathcal{P}(S \setminus \{a\})$ the factor algebra B/I

Exercise 30 Given a topological space (X, τ) , the following conditions are equivalent for all $x, y \in X$.

1. $\{x\}^a \subseteq \{y\}^a$.
2. $x \in \{y\}^a$.
3. $x \in U$ implies $y \in U$ for all open sets U .

Exercise 31 Characterize those ideals I in a Boolean algebra B for which the factor algebra B/I consists of exactly two elements.

Exercise 32 Let $\emptyset \neq \mathcal{A} \subseteq \mathcal{P}(S)$ be a finite family of sets with $S \in \mathcal{A}$, say $\mathcal{A} = \{A_1, \dots, A_n\}$. Define $A_T := \bigcap_{i \in T} A_i \cap \bigcap_{i \notin T} S \setminus A_i$ for $T \subseteq \{1, \dots, n\}$.

1. $\mathcal{P} := \{A_T \mid \emptyset \neq T \subseteq \{1, \dots, n\}, A_T \neq \emptyset\}$ forms a partition of S .
2. $\{\bigcup \mathcal{P}_0 \mid \mathcal{P}_0 \subseteq \mathcal{P}\}$ is the smallest set algebra over S which contains \mathcal{A} .

Exercise 33 As in Example 1.105 on page 46 let $X := \{0, 1\}^{\mathbb{N}}$ be the space of all infinite sequences. Put

$$\mathcal{C} := \{A \times \prod_{j>k} \{0, 1\} \mid k \in \mathbb{N}, A \in \mathcal{P}(\{0, 1\}^k)\}.$$

Show that \mathcal{C} is an algebra.

Exercise 34 Let X and \mathcal{C} be as in Exercise 33. Show that

$$\mu(A \times \prod_{j>k} \{0, 1\}) := \frac{|A|}{2^k}$$

defines a monotone and countably additive map $\mu : \mathcal{C} \rightarrow [0, 1]$ with $\mu(\emptyset) = 0$.

Exercise 35 Show that a countably subadditive and monotone set function on a set algebra is additive.

1.11 Solutions

Solution for Exercise 1 $\langle a, b \rangle = \langle a', b' \rangle$ iff $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$. If $\{a\} = \{a'\}$, we have $a = a'$, so that $\{a, b\} = \{a', b'\}$ implies $\{a, b\} = \{a, b'\}$. If $a = b$, this implies $a' = a = b'$, otherwise we obtain $b = b'$. If, on the other hand, $\{a\} = \{a', b'\}$, then $a = a' = b'$, and then $\{a'\} = \{a, b\}$ implies $a = a' = b$. In any case, $\langle a, b \rangle = \langle a', b' \rangle$ implies $a = a'$ and $b = b'$. The converse is trivial.

Solution for Exercise 2 If f is injective, $X = f^{-1}[f[X]]$ for all $X \subseteq A$, hence f^{-1} is surjective. If f is not injective, we find $a, a' \in A$ with $a \neq a'$ and $b := f(a) = f(a')$. Hence $\{a, a'\} = f^{-1}[\{b\}]$, so that neither $\{a\}$ nor $\{a'\}$ are inverse images under f^{-1} . Thus f^{-1} is not surjective.

If f is surjective, $Y = f[f^{-1}[Y]]$ for all $Y \subseteq B$, hence $f^{-1}[Y] = f^{-1}[Y']$ implies $Y = f[f^{-1}[Y]] = f[f^{-1}[Y']] = Y'$. Conversely, if f^{-1} is injective, we conclude from $f^{-1}[f[A]] = f^{-1}[B]$ that $f[A] = B$.

Solution for Exercise 3 If p is prime, p has no smaller divisor than itself in $\mathbb{N} \setminus \{1\}$. If, on the other hand, p is minimal in $\mathbb{N} \setminus \{1\}$, and if p can be written as $p = a \cdot b$ with $a, b \in \mathbb{N} \setminus \{1\}$, then both a and b are strictly \leq_d -smaller than p .

Solution for Exercise 4 $B := \mathbb{N} \setminus \{1\}$ is an upper bound for A , since $\{2 \cdot n, 2 \cdot n + 1\} \subseteq B$ for all $n \in \mathbb{N}$. B is also the smallest upper bound, because each upper bound must contain all $n \geq 2$.

Solution for Exercise 5 Let $\mathcal{Q} := \{X \in \mathcal{P}(S) \mid X \subseteq H(X)\}$. If $X \in \mathcal{Q}$, then $X \subseteq A$, hence $X \subseteq H(X) \subseteq H(A)$, so that $H(A)$ is an upper bound to \mathcal{Q} . This means $A \subseteq H(A)$, hence $A \in \mathcal{Q}$, so that $H(A) \subseteq A$. Hence A is a fixed point of H . Let Y be another fixed point for \mathcal{Q} , then $Y \in \mathcal{Q}$, thus $Y \subseteq A$.

This is a variant of the *Knaster-Tarski Fixed point Theorem*.

Solution for Exercise 6 Put $H(A) := X \setminus g[Y \setminus f[A]]$, then $H : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ is order preserving. Let $X_1 := A$ be the maximal fixed point to H , and put $Y_1 := f[A]$, then $X \setminus A = g[Y \setminus Y_1]$, thus $X_2 := X \setminus X_1$ and $Y_2 := Y \setminus Y_1$ have the desired properties.

Solution for Exercise 7 Let $f : A \rightarrow B$ and $g : B \rightarrow A$ be injective maps. Decompose $A = A_1 \cup A_2$ with disjoint A_1, A_2 and $B = B_1 \cup B_2$ with disjoint B_1, B_2 such that $f[A_1] = B_1$ and $g[B_2] = A_2$ according to Exercise 6. Note that given $a \in A_2$ there exists $b \in B_2$ with $g(b) = a$; because g is injective, b is unique. Denote b by $g^{-1}(a)$. Then define $h : A \rightarrow B$ through

$$h(x) := \begin{cases} f(x), & x \in A_1, \\ g^{-1}(x), & x \in A_2. \end{cases}$$

It is plain that h is injective. Let $b \in B_1$, then $b = f(a)$ for some $a \in A_1$; if $b \in B_2$, $g(b) \in A_2$, and $h(g(b)) = b$ by construction. Thus h is onto as well.

Solution for Exercise 8 Given $x \in \mathbb{N}_0$, there exists a unique $\langle a, b \rangle \in \mathbb{N}_0 \times \mathbb{N}_0$ so that $J(a, b) = x$. Define $K(x) := a$, then $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ is well defined: if $J(a', b') = x$, then because J is injective $\langle a, b \rangle = \langle a', b' \rangle$, in particular $a = a'$. It is also clear from the construction that $K(x) \leq x$ holds. Since $K = \pi_1 \circ J^{-1}$ with π_1 as the projection to the first component, and since both π_1 and J^{-1} are surjective, K is surjective. Similarly, $L(x) := b$ iff $J(a, b) = x$ for some $a \in \mathbb{N}_0$. Then the desired properties for L are inferred in the same way. It is obvious that $J(K(x), L(x)) = x$ always holds.

Solution for Exercise 10 Let $N_2 := \{\{a, b\} \mid a, b \in \mathbb{N}, a \neq b\}$ all subsets of \mathbb{N} with exactly two elements, define $P_2 := \{\langle x, y \rangle \mid x, y \in \mathbb{N}, x < y\}$, then $h : X \mapsto \langle \min X, \max X \rangle$ is an injective map $N_2 \rightarrow P_2$; the Cantor map $J : P_2 \rightarrow \mathbb{N}$ restricted to P_2 is injective as well by Proposition 1.3, thus $J \circ h : N_2 \rightarrow \mathbb{N}$ is injective. On the other hand, $n \mapsto \{n, n+1\}$ is injective $\mathbb{N} \rightarrow N_2$.

Now let $k > 2$ and put

$$N_k := \{A \subseteq \mathbb{N} \mid A \text{ has exactly } k \text{ elements}\},$$

$$P_k := \{\langle x_1, \dots, x_k \rangle \mid x_1, \dots, x_k \in \mathbb{N}, x_1 < x_2 < \dots < x_k\}.$$

Define $\gamma_k : N_k \rightarrow P_k$ inductively by $\gamma_2 := h$, and $\gamma_{k+1}(A) := \gamma_k(A \setminus \{\max A\}) \frown \max A$. Then γ_k is an injection, so that $\tau_k \circ \gamma_k : N_k \rightarrow \mathbb{N}$ is an injection, where τ_k is defined in Proposition 1.4. On the other hand, $n \mapsto \{n, n+1, \dots, n+(k-1)\}$ is an injective map $\mathbb{N} \rightarrow N_k$.

By using Proposition 1.5 it is shown that the set of all finite subsets is countable without making use of $(\mathbb{A}\mathbb{C})$.

Solution for Exercise 11 Every element of ω_1 is an ordinal, hence a set, thus ① holds. Let $\alpha \in \omega_1$, then $\alpha = \{\zeta \mid \zeta < \alpha\} \subseteq \omega_1$, giving property ②. Since each set of ordinals is well-ordered by \in , we see that property ③ holds. If finally $\emptyset \neq B \subseteq \omega_1$, then B has a smallest element ζ . If $\eta \in \zeta \cap B$, ζ would not be the smallest element of B , since $\eta \in \zeta$ would be strictly smaller. If ω_1 is countable, we have $\omega_1 \in \omega_1$, this contradicts Lemma 1.31.

Solution for Exercise 13 The associate law both for \ominus and \cap follows by direct computation. The neutral element of \ominus is \perp , and $a \ominus a = \perp$, so each element is inverse to itself. $a \ominus b = b \ominus a$ is obvious. Thus (B, \ominus) is an Abelian group. Since $a \wedge (b \ominus c) = a \wedge b \ominus a \wedge c$ and $(b \ominus c) \wedge a = b \wedge a \ominus c \wedge a$, we conclude that (B, \ominus, \wedge) is a commutative ring.

Solution for Exercise 14 Let \mathcal{G} be a family of finite character, every chain \mathcal{C} in \mathcal{G} has an upper bound: We find for each finite set $\{x_1, \dots, x_n\} \subseteq \bigcup \mathcal{C}$ a set $C \in \mathcal{C}$ with $\{x_1, \dots, x_n\} \subseteq C$. Hence $\{x_1, \dots, x_n\} \subseteq \bigcup \mathcal{C}$, hence every finite subset of $\bigcup \mathcal{C}$ is in $\bigcup \mathcal{C}$. By Zorn's Lemma there exists a maximal element \mathcal{M} for \mathcal{G} . Hence the assertion follows from Proposition 1.42.

Solution for Exercise 15 Put $I := L \setminus F$. “ \Rightarrow ” If $a \in I$ and $b \in I$, we have $a \in F$ or $b \in F$ is false, hence $a \vee b \in F$ is false, thus $a \vee b \in I$. $a \in I$ means $a \notin F$, thus $b \leq a$ implies $b \notin F$. Similarly, $a \wedge b \in I$ implies $a \in I$ and $b \in I$. Thus I is an ideal. “ \Leftarrow ” is done in the same way.

Solution for Exercise 16 Assume that $\gamma = x \in V$, then the assertion is trivial. Let the assertion be true for φ_1 and for φ_2 . Then $v^* \models \varphi_1 \wedge \varphi_2$ iff $v^* \models \varphi_1$ and $v^* \models \varphi_2$. The induction hypothesis yields that this is equivalent to $\varphi_1 \in \mathcal{M}^*$ and $\varphi_2 \in \mathcal{M}^*$. Assume that $\varphi_1 \wedge \varphi_2 \notin \mathcal{M}^*$ then the construction of \mathcal{M}^* implies that $\neg(\varphi_1 \wedge \varphi_2) \in \mathcal{M}^*$, since $\varphi_1 \wedge \varphi_2$ is a formula, hence has to be considered at some time. But this implies $v^*(\varphi_1 \wedge \varphi_2) = 0$, contradicting the assumption. The converse implication is trivial. Now assume that the assertion is true for formula φ . If $v^* \models \neg\varphi$, then $v^*(\varphi) = 0$, hence $\varphi \notin \mathcal{M}^*$, thus, again by construction, $\neg\varphi \in \mathcal{M}^*$.

Solution for Exercise 18 Assume $A := \{s_1, \dots, s_n\} \in \mathcal{F}$ for some $n \in \mathbb{N}$. If $\{s_i\} \notin \mathcal{F}$ for all i , $1 \leq i \leq n$, then $S \setminus \{s_i\} \in \mathcal{F}$ for all i , hence $S \setminus A \in \mathcal{F}$, a contradiction.

Solution for Exercise 19

- $D \wedge E = B; D \vee E = L; (J \wedge L) \wedge K = D \wedge K = D$.
- $(L \wedge E) \wedge K = B \wedge B; L \wedge (E \wedge K) = L \wedge B = B; C \wedge E = \perp$.
- $(C \vee D) \vee E = F \vee E = J; \sup\{C, D, E\} = \top; C \vee (D \vee E) = C \vee L = \top$.
- $J \wedge (L \vee K) = J \wedge \top = J; (J \wedge L) \vee (J \wedge K) = H \vee F = J; C \vee G = K$.

Solution for Exercise 20 If L is finite, $b = \sup\{a \in L \mid a \leq b\}$. Thus if s is join irreducible, we can find exactly one element covering s . The converse is trivial.

Solution for Exercise 21 Assume $I := \{s \in P \mid s \leq t\} = I_1 \cup I_2$ with $I_1, I_2 \in \mathcal{D}(P)$. Assume $t \in I_1$, and let $s \in I_2$, then $s \leq t$, hence $s \in I_1$, thus $I_2 \subseteq I_1$. Conversely, if $I = \bigcup_{t \in I} \{s \in P \mid s \leq t\}$ is join irreducible, we find $t \in I$ such that $I = \{s \in P \mid s \leq t\}$, since P is finite.

Solution for Exercise 22 The singleton sets $\{x\}$ are join-irreducible in $\mathcal{P}(S)$. The lattice of all open intervals in \mathbb{R} does not have any irreducible elements.

Solution for Exercise 23 Assume that $(x \vee y) \wedge z = (z \wedge y) \vee (z \wedge x)$ holds, then

$$\begin{aligned}
 (x \vee y) \wedge (x \vee z) &= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) \\
 &= x \vee ((x \vee y) \wedge z) \\
 &= x \vee ((z \wedge y) \vee (z \wedge x)) \\
 &= x \vee (y \wedge z)
 \end{aligned}$$

Solution for Exercise 24 Let $\langle x, y \rangle \leq \langle x', y' \rangle$ iff $x \leq x'$ and $y \leq y'$ for $\langle x, y \rangle, \langle x', y' \rangle \in \mathbb{R}_+ \times \mathbb{R}_+$. Then $\{\langle 0, x \rangle \mid x \in \mathbb{R}_+\} \cup \{\langle x, 0 \rangle \mid x \in \mathbb{R}_+\}$ is a down set. It is not an ideal, since it contains $\langle 0, 1 \rangle$ and $\langle 1, 0 \rangle$, but not $\langle 1, 1 \rangle = \langle 0, 1 \rangle \vee \langle 1, 0 \rangle$.

Solution for Exercise 25

$$\begin{aligned} x &= x \wedge (c \vee x) &= x \wedge (c \vee y) &= (x \wedge c) \vee (x \wedge y) \\ &= (y \wedge c) \vee (x \wedge y) &= y \wedge (c \vee x) &= y \wedge (c \vee y) \\ &= y \end{aligned}$$

Solution for Exercise 26 The intersection $K \cap L$ of two subgroups K and L is a subgroup again. Put

$$K + L := \{a + b \mid a \in K, b \in L\}.$$

This is a subgroup of G : if $g = a + b, g' = a' + b' \in K + L$, then $g - g' = (a - a') + (b - b') \in K + L$. It is clear that $K \subseteq K + L, L \subseteq K + L$, on the other hand, if $H \subseteq G$ is a subgroup with $K \subseteq H, L \subseteq H$, then $K + L \subseteq H$, so that $K + L$ is indeed the smallest subgroup containing K and L . Hence define

$$\begin{aligned} K \wedge L &:= K \cap L, \\ K \vee L &:= K + L, \end{aligned}$$

then the set of all subgroups is a lattice.

It could be noted that a very similar argument applies to the normal subgroups in an arbitrary group (a subgroup H is called *normal* iff $\forall a \in G : aH = Ha$ holds).

Solution for Exercise 27 Put $d := (a \wedge b) \vee (a \wedge c)$ and consider $d : a$. We have $a \wedge b \leq d$ and $a \wedge c \leq d$, hence $b \leq d : a$ and $c \leq d : a$. Thus $b \wedge c \leq d : a$, which implies $a \wedge (b \vee c) \leq a \wedge (d : a) \leq d = (a \wedge b) \vee (a \wedge c)$. Because $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$ always holds, distributivity is established (see Exercise 23).

Define the pseudo-complement in a Boolean algebra through $b : a := -a \vee b$, then it is easily seen that the defining properties hold.

Solution for Exercise 28 The first assertion follows from the observation that

$$\sup A = \inf\{b \in L \mid b \text{ is an upper bound to } A\}.$$

The set of all equivalence relations on a set X has $\{\langle x, x \rangle \mid x \in X\}$ as the smallest and $X \times X$ as the largest element. The second assertion follows from the first one after having seen that the intersection of an arbitrary set of equivalence relations on X is an equivalence relation and its greatest lower bound.

Solution for Exercise 29 Given $X, Y \in B$, we have $X \sim_I Y$ iff either both X and Y contain a or both don't. Consequently, $B/I = \{\top, \perp\}$.

Solution for Exercise 30 $1 \Rightarrow 2$: This follows from $x \in \{x\}^a$.

$2 \Rightarrow 3$: If $x \in U$, but $y \notin U$ for some open set U , we would have $\{y\}^a \subseteq X \setminus U$, contradicting the assumption.

$3 \Rightarrow 1$: Let $y \in F$ for some closed set F , then $y \notin X \setminus F$, hence $x \notin X \setminus F$ by assumption, thus each closed set which contains y contains x as well. This implies $\{x\}^a \subseteq \{y\}^a$.

This indicates a first connection of topology and order. Define $x \leq y$ iff $x \in \{y\}^a$, then this relation is certainly reflexive and transitive; if (X, τ) has the additional property that given $x \neq y$ there exists an open set containing exactly one of them, then \leq is also antisymmetric.

Solution for Exercise 31 $B/I = \{\top_I, \perp_I\}$ iff I is a prime ideal. " \Rightarrow " A prime ideal K extending I is $K = \{x \in B \mid [x]_{\sim_I} \in \perp_I\} = I$ according to Theorem 1.85. " \Leftarrow " A prime ideal is maximal by Lemma 1.79, hence the factor algebra must be trivial by Theorem 1.85.

Solution for Exercise 32 The A_T are mutually disjoint by construction, and their union is S , since $S \in \mathcal{A}$. Put $\mathcal{C} := \{\bigcup \mathcal{P}_0 \mid \mathcal{P}_0 \subseteq \mathcal{P}\}$, then $\emptyset \in \mathcal{C}$, and $S \setminus (\bigcup \mathcal{P}_0) = \bigcup \mathcal{P}(\{1, \dots, n\}) \setminus \mathcal{P}_0$ computes the complement of a set in \mathcal{C} . Since $\bigcup \mathcal{P}_0 \cup \bigcup \mathcal{P}_1 = \bigcup (\mathcal{P}_0 \cup \mathcal{P}_1)$ and $\bigcup \mathcal{P}_0 \cap \bigcup \mathcal{P}_1 = \bigcup (\mathcal{P}_0 \cap \mathcal{P}_1)$, \mathcal{C} is closed under the algebra operations. Since the algebra generated by \mathcal{A} must contain \mathcal{C} , the assertion follows.

Solution for Exercise 33 It is clear that $X \in \mathcal{C}$ and $\emptyset \in \mathcal{C}$ hold. Let $D, E \in \mathcal{C}$, then $D = A \times \prod_{j>k} \{0, 1\}$, $E = B \times \prod_{j>\ell} \{0, 1\}$ with $A \subseteq \{0, 1\}^k$, $B \subseteq \{0, 1\}^\ell$. Assume $k \geq \ell$ (if $k \leq \ell$ the argument is the same), then $E = B' \times \prod_{j>k} \{0, 1\}$ with $B' := B \times \{0, 1\}^{k-\ell} \subseteq \{0, 1\}^k$, thus $D \cap E = (A \cap B') \times \prod_{j>k} \{0, 1\} \in \mathcal{C}$. Hence \mathcal{C} is closed under finite intersections. Since $X \setminus (A \times \prod_{j>k} \{0, 1\}) = (\{0, 1\}^k \setminus A) \times \prod_{j>k} \{0, 1\}$ for $A \subseteq \{0, 1\}^k$, \mathcal{C} is closed under complementation as well.

Solution for Exercise 34 Assume that

$$A \times \prod_{j>k} \{0, 1\} = A' \times \prod_{j>\ell} \{0, 1\},$$

with $k \leq \ell$, then $A' = A \times \{0, 1\}^{\ell-k}$, so that

$$\frac{|A'|}{2^\ell} = \frac{|A|}{2^k} \cdot \frac{2^{\ell-k}}{2^{\ell-k}} = \frac{|A|}{2^k}.$$

Thus μ is well-defined. $\mu(\emptyset) = 0$ is trivial; since $A \subseteq B$ implies $|A| \leq |B|$ and $|A \cup B| = |A| + |B|$, if A and B are disjoint, μ is monotone and additive. Countable additivity is vacuously satisfied.

Solution for Exercise 35 Let \mathcal{C} be a set algebra, $\mu : \mathcal{C} \rightarrow [0, \infty]$ monotone and additive. If $\bigcup_{n \in \mathbb{N}} A_n =: A \in \mathcal{C}$, then $A = \bigcup_{n \in \mathbb{N}} B_n$ with $B_1 := A_1$ and $B_{n+1} := A_{n+1} \setminus (\bigcup_{i=1}^n A_i)$ (this is sometimes called the *first entrance trick*). The B_n are mutually disjoint, and $B_n \in \mathcal{C}$, because \mathcal{C} is an algebra. Thus $\mu(A) = \sum_{i=1}^{\infty} \mu(B_i) \leq \sum_{i=1}^{\infty} \mu(A_i)$.

References

- [Acz00] A. D. Aczel. *The Mystery of the Aleph - Mathematics, the Kabbalah and the Search for Infinity*. Pocket Books, New York, 2000.
- [Aum54] G. Aumann. *Reelle Funktionen*. Springer-Verlag, Berlin, Göttingen, Heidelberg, 1954.
- [Bar77] J. Barwise, editor. *Handbook of Mathematical Logic*. North-Holland Publishing Company, Amsterdam, 1977.
- [Bil95] P. Billingsley. *Probability and Measure*. John Wiley & Sons, New York, third edition edition, 1995.
- [Bir67] G. Birkhoff. *Lattice Theory*, volume 25 of *Colloquium Publications*. American Mathematical Society, Providence, RI, 1967.
- [BN98] F. Baader and T. Nipkow. *Term rewriting and all that*. Cambridge University Press, Cambridge, UK, 1998.
- [Bog07] V. I. Bogachev. *Measure Theory*. Springer-Verlag, 2007.
- [Bro08] T. J. Bromwich. *In Introduction to the Theory of Infinite Series*. MacMillan and Co., London, 1908.
- [Chr64] G. Chrystal. *Textbook of Algebra I/II*. Chelsea Publishing Company (Reprint), New York, 1964.
- [CLR92] T. H. Cormen, C. E. Leiserson, and R. L. Rivest. *An Introduction to Algorithms*. The MIT Press, Cambridge MA, 1992.
- [COP01] D. Cantone, E. G. Omodeo, and A. Policriti. *Set Theory for Computing*. Springer-Verlag, Berlin, Heidelberg, New York, 2001.
- [Dav00] M. Davis. *Engines of Logic - Mathematics and the Origin of the Computer*. W. W. Norton, New York, London, 2000.
- [DF89] E.-E. Doberkat and D. Fox. *Software Prototyping mit SETL*. Leitfäden und Monographien der Informatik. Teubner-Verlag, Stuttgart, 1989.
- [DP02] B.A. Davey and H. A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, Cambridge, UK, 2002.
- [Els99] J. Elstrodt. *Maß- und Integrationstheorie*. Springer-Verlag, Berlin-Heidelberg-New York, 2 edition, 1999.
- [Fic64] G. M. Fichtenholz. *Differential- und Integralrechnung I-III*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1964.
- [Gol96] D. Goldrei. *Classic Set Theory*. Chapman and Hall/CRC, Boca Raton, 1996.
- [Gol12] R. Goldblatt. Topological proofs of some Rasiowa-Sikorski lemmas. *Studia Logica*, 100:1 – 18, 2012.

- [Her06] H. Herrlich. *Axiom of Choice*. Number 1876 in Lect. Notes Math. Springer-Verlag, Berlin, Heidelberg, New York, 2006.
- [HS65] E. Hewitt and K. R. Stromberg. *Real and Abstract Analysis*. Springer-Verlag, Berlin, Heidelberg, New York, 1965.
- [Jec73] T. Jech. *The Axiom of Choice*, volume 75 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Company, New York, 1973.
- [Jec06] T. Jech. *Set Theory*. Springer-Verlag (The Third Millennium Edition), Berlin, Heidelberg, New York, 2006.
- [KM76] K. Kuratowski and A. Mostowski. *Set Theory*, volume 86 of *Studies in Logic and the Foundations of Mathematics*. North-Holland and PWN, Polish Scientific Publishers, Amsterdam and Warszawa, 1976.
- [Knu73] D. E. Knuth. *The Art of Computer Programming. Vol. I, Fundamental Algorithms*. Addison-Wesley, Reading, Mass., 2 edition, 1973.
- [MS64] J. Mycielski and S. Swierczkowski. On the Lebesgue measurability and the axiom of determinateness. *Fund. Math.*, 54:67 – 71, 1964.
- [OGS09] B. O’Sullivan, J. Goerzen, and D. Stewart. *Real World Haskell*. O’Reilly, Sebastopol, CA, 2009.
- [SDDS86] J. T. Schwartz, R. B. K. Dewar, E. Dubinsky, and E. Schonberg. *Programming with Sets — An Introduction to SETL*. Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1986.
- [Sta97] R. Stanley. *Enumerative Combinatorics*, volume 1 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, UK, 1997.
- [Tay99] P. Taylor. *Practical Foundations of Mathematics*, volume 59 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1999.
- [Thi65] C. Thiel. *Sinn und Bedeutung in der Logik Gottlob Freges*. Verlag Anton Hain, Meisenheim am Glan, 1965.